

ALI-ELI PRINCIPLES FOR A DATA ECONOMY - DATA TRANSACTIONS AND DATA RIGHTS -

ELI Final Council Draft
Neil Cohen and Christiane Wendehorst

SUBJECTS COVERED

1	REPORTERS' MEMORANDUM	3
2	Introductory Note	6
3	Part I: General Provisions	14
4	Principle 1: Purpose of these Principles	14
5	Principle 2: Scope of these Principles	22
6	Principle 3: Definitions	27
7	Principle 4: Remedies	43
8	Part II: Data Contracts	48
9	Chapter A: Rules and Principles Governing Data Contracts	48
10	Principle 5: Application of these Principles to data contracts	48
11	Principle 6: Interpretation and application of contract law	53
12	Chapter B: Contracts for Supply or Sharing of Data	56
13	Principle 7: Contracts for the transfer of data	56
14	Principle 8: Contracts for simple access to data	72
15	Principle 9: Contracts for exploitation of a data source	78
16	Principle 10: Contracts for authorization to access	84
17	Principle 11: Contracts for data pooling	89
18	Chapter C: Contracts for Services with regard to Data	95
19	Principle 12: Contracts for the processing of data	95
20	Principle 13: Data trust contracts	103
21	Principle 14: Data escrow contracts	114
22	Principle 15: Data marketplace contracts	120
23	Part III: Data Rights	125

Principles for a Data Economy

1	Chapter A: Rules and Principles Governing Data Rights	125
2	Principle 16: Data rights	125
3	Principle 17: Application of these Principles to data rights	130
4	Chapter B: Data Rights with Regard to Co-Generated Data	134
5	Principle 18: Co-generated data	134
6	Principle 19: General factors determining rights in co-generated data	140
7	Principle 20: Access or porting with regard to co-generated data	146
8	Principle 21: Desistance from data activities with regard to co-generated data	156
9	Principle 22: Correction of co-generated data	161
10	Principle 23: Economic share in profits derived from co-generated data	163
11	Chapter C: Data Rights for the Public Interest	167
12	Principle 24: Justification for data rights and obligations	167
13	Principle 25: Granting of data access by the controller	174
14	Principle 26: Data activities by recipient	178
15	Principle 27: Reciprocity	183
16	Part IV: Third Party Aspects of Data Activities	185
17	Chapter A: Protection of Others against Data Activities	185
18	Principle 28: Wrongfulness of data activities vis-à-vis another party	185
19	Principle 29: Rights that have third-party effect per se	191
20	Principle 30: Contractual limitations	197
21	Principle 31: Unauthorized access	202
22	Chapter B: Effects of Onward Supply on the Protection of Others	206
23	Principle 32: Duties of a supplier in the context of onward supply	206
24	Principle 33: Direct action against downstream recipient	214
25	Principle 34: Wrongfulness taking effect vis-à-vis downstream recipient	218
26	Chapter C: Effects of Other Data Activities on the Protection of Third Parties	228
27	Principle 35: Duties of a controller with regard to data processing and derived data	228
28	Principle 36: Wrongful processing	234
29	Principle 37: Effect of non-material non-compliance	240
30	Part V: Multi-State Issues	244
31	Principle 38: Application of established choice-of-law rules of the forum	244
32	Principle 39: Issues not covered by established choice of law rules of the forum	251
33	Principle 40: Relevance of storage location	255
34	BLACKLETTER OF ELI FINAL COUNCIL DRAFT	261

1 **Please note that this document is a Draft which has not yet been approved by the ELI**
2 **Membership and does not yet represent the official position of the ELI.**

3 **REPORTERS' MEMORANDUM**

4 Discussions about a joint project between the American Law Institute (ALI) and the
5 European Law Institute (ELI) in the field of the data economy started in 2016. Meetings with a
6 view to conducting a mapping exercise included workshops in October 2016 in New York and in
7 March 2017 in Vienna. A 'Draft Framework for Discussion' dated 25 August 2017 by CHRISTIANE
8 WENDEHORST, NEIL COHEN and STEVE WEISE was presented at the ELI Annual Conference in
9 Vienna on 7 September 2017. This document was intended to demonstrate that it is both feasible
10 and timely to formulate ALI-ELI Principles for a Data Economy, presenting a first tentative draft
11 of what such Principles could look like. The project was adopted by the ALI Council on 19 January
12 2018 and by the ELI Council on 9 February 2018, appointing NEIL COHEN and CHRISTIANE
13 WENDEHORST as Reporters, and STEVE WEISE and THE LORD JOHN THOMAS OF CWMGIEDD as
14 Chairs coordinating a wider group of advisers from both the ALI and the ELI.

15 Members of this group convened in New York on 15 and 16 February 2018 to advise the
16 Reporters concerning the overall direction of the project. The Reporters produced a 'Pre-Draft'
17 dated 20 August 2018 that was presented at the ELI Annual Conference in Riga on 6 September
18 and discussed in detail with ELI Advisors and the ELI Members Consultative Committee (MCC)
19 on 8 September 2018. Considering guidance received at this meeting the document was submitted
20 as 'Preliminary Draft No. 1' to the ALI Advisors and Members Consultative Group (MCG) in
21 Philadelphia on 25 and 26 October 2018. Both meetings together resulted in a broad range of
22 changes, including a re-ordering of the Parts and a clearer focus on the transactional aspects,
23 reflected in 'Preliminary Draft No. 2', dated 4 February 2019, and discussed at a joint meeting with
24 the ALI and ELI Advisors and MCG/MCC in Philadelphia on 22 February 2019. An interim
25 'Preliminary Draft No. 2bis' was discussed with ELI Advisors and MCC in Vienna on 3 September
26 2019, resulting in 'Preliminary Draft No. 3', which was completed on 15 October and discussed
27 with ALI Advisors and MCG in Philadelphia on 31 October 2019. It took on board guidance
28 received since the earlier 2019 meetings, including scrutiny undertaken by the Berlin based tech-

1 company acs-plus GmbH, suggestions from the industry, and inspirations gained at a meeting
2 hosted jointly by UNCITRAL and French governmental institutions in Paris on 15 March 2019 as
3 well as at the 52nd Commission session of UNCITRAL in Vienna on 17 July 2019. It also took on
4 board inspiration gained from other international sources such as the Contract Guidelines on
5 Utilization of AI and Data (Data Section) from June 2018, issued by the Japanese Ministry of
6 Economy, Trade and Industry (referred to as ‘METI Guidelines’) as well as the first report on
7 collected model contract terms of the Support Centre for Data Sharing which was initiated by the
8 European Commission in early 2019.

9 On the basis of guidance received at and after the 31 October 2019 meeting, Principles 1-
10 10 and 16-23 (then 15-22) were submitted as ‘ALI Council Draft No. 1’ to the ALI Council for its
11 meeting on 17 January 2020 and approved that day. Taking on board further guidance received by
12 ALI and ELI members, by UNCITRAL Working Group No. IV on Electronic Commerce on 28
13 November 2019, by the participants of a conference hosted by the German Ministry of Justice on
14 12 and 13 December 2019 in Berlin, the ELI Council on 21 and 21 February 2020 and the
15 participants of an expert workshop hosted by UNCITRAL and Unidroit on 10 and 11 March 2020
16 in Vienna, the Reporters produced ‘Tentative Draft No. 1’. The latter was submitted electronically
17 for consultation to the Members of the ALI, in lieu of submission for approval at the 2020 Annual
18 Meeting (cancelled due to the COVID-19 situation). Tentative Draft No. 1 was further submitted
19 to the members of the ELI Advisors and MCC for their remote meeting on 22 June 2020. The
20 guidance received led to the production of ‘Preliminary Draft No. 4’, which was presented to the
21 ELI Members at the ELI Annual Conference on 10 September 2020 and later discussed with ALI
22 and ELI Advisors and MCG/MCC at a remote meeting on 8 October 2020. With the feedback
23 received, including the feedback received at an international conference co-hosted by UNCITRAL
24 and the Japanese government on 10 September 2020, from members of the Data Governance
25 Working Group of the Global Partnership on AI (GPAI), as well as from the Federation of German
26 Industries at a meeting on 4 December 2020, the Reporters produced ‘Council Draft No. 2’, which
27 was submitted to the ALI Council for its meeting on 21 January 2021 and approved that day.

28 Taking on board guidance received during the ALI Council meeting, a joint meeting with
29 the ALI and ELI Advisors and MCG/MCC on 8 February, and the meeting of the ELI Council on
30 11 February 2021, the Reporters produced Tentative Draft No. 2 which was submitted to the ALI
31 Membership for its remote Annual Meeting 2021 on 18 May 2021.

1 After the approval by the ALI Membership and a joint meeting held with the ALI and ELI
2 Advisors and MCG/MCC on 28 June 2021, the Reporters produced this ‘ELI Final Council Draft’
3 which was submitted to the ELI Council for their meeting on 1 September 2021. After the approval
4 by the ELI Council, this draft was submitted to the ELI Membership for their approval until 24
5 September 2021.

6 On the European side, the project is generously
7 funded by the Fritz Thyssen Foundation



1 This focus on binary impulses in large batches, which may be stored, transmitted, processed with
2 the help of machines, etc., is also what differentiates transactions in the data economy from
3 traditional information services. Where A pays B for gathering information on election outcomes
4 in a foreign country the focus is on B *doing* something (i.e. telling A, even if A and B have agreed
5 B must give A the information in a particular format, such as by email). By contrast, where A pays
6 B for real time transmission of exit poll data to be displayed on A's news channel the focus is on
7 B *delivering* something (i.e. a large batch of binary impulses with a particular meaning in a
8 particular format).

9 The fact that data is different is the reason why it has become necessary to draft principles
10 for data transactions and data rights instead of merely referring to the existing law of, say, sale and
11 lease of goods, or of services. It is important to note that the legal analysis depends to a great degree
12 on whether the relevant data is protected under rules such as intellectual property law or trade secret
13 law and/or rules that limit certain types of conduct (such as data privacy/data protection law and
14 consumer protection law).

15 This project seeks to propose a set of principles that might be implemented in any kind of
16 legal environment, and to work in conjunction with any kind of data privacy/data protection law,
17 intellectual property law or trade secret law, without addressing or seeking to change any of the
18 substantive rules of these bodies of law.

19 **B. Players and relations in the data ecosystem**

20 These Principles cannot provide a complete set of standards for any sort of dealings within
21 the data economy. This is so for a variety of reasons, including the special dynamics of the data
22 economy as a fast-moving field, the desire to reduce complexity and focus the Principles on some
23 central points, and the need to produce something that works in vastly differing legal environments
24 in different regions of the world.

25 The Principles have taken the basic types of players and relations which we find in data
26 ecosystems as a starting point. The central player in all data ecosystems is the controller (often also
27 called the 'holder') of data, i.e. the party that is in a position to access the data and that decides
28 about the purposes and means of their processing. That controller may exercise control all by itself
29 or share it with co-controllers, such as under a data pooling arrangement. A (mere) processor of
30 data, on the other hand, is a service provider that processes data on a controller's behalf.

1 There is also a variety of different parties contributing in different ways to the generation
2 of data. One important way of contributing to the generation of data is by being the individual or
3 legal entity that is the subject of the information recorded in the data. Another way of contributing
4 to the generation of data is by being a data producer, i.e. generating data in the sense of recording
5 information that had previously not been recorded. There are also parties that do not produce data
6 in this sense, but create added value by assembling data in some meaningful ways, and parties that
7 contribute in more remote roles. The parties that contribute to the generation of data may provide
8 the data to the controller (provided data). Data may be produced by the controller itself through
9 observing the parties (observed data). The controller may also obtain derived or inferred data from
10 data that has been observed or provided.

11 A controller of data often supplies the data to third party data recipients, in particular under
12 contractual or other data sharing arrangements. Recipients of data may become new controllers
13 where data is fully transferred to them, or they may receive only access to the data, such as where
14 they are permitted to process data with a mobile software agent on the supplier's server. Needless
15 to say, an important part of the data economy consists in using data for creating new value, such as
16 by developing and marketing data-based products and services; marketing these products and
17 services is, however, not covered by these Principles.

18 In addition to the parties mentioned there is an increasing number of different types of data
19 intermediaries, such as data trustees, data escrowees, or data marketplace providers. They facilitate
20 the transactions between the different actors, in particular between parties generating data and data
21 controllers, and between data suppliers and data recipients, such as by acting as trusted third party.
22

1 Chapter B is more specifically about contracts for supply or sharing of data. The Principles
2 identify, as a first step, typical contractual promises in the data economy that involve different
3 types and modalities of provision of data and show how these transactions in the data economy can
4 be systematized, with a view to analysing the rights and obligations of the parties to the transaction.
5 These rights and obligations may be very different, depending on whether, *e.g.*, a party has
6 promised to fully transfer data to a medium within the recipient’s sphere of control, or only to grant
7 access to a medium on which data is stored or maybe even only to consent to the collecting and
8 processing of data by the other party to the transaction while refusing to take any responsibility for
9 what the other party ultimately receives. Where data is not just provided by a supplier to a recipient,
10 but where two or several parties decide to contribute data to a data pool or closed platform each of
11 them has access to, this again may require a somewhat different set of rules. It should be noted that
12 the terms ‘supply’ and ‘sharing’ may, by and large, be used interchangeably, even though ‘supply’
13 fits better to describe a one-way provision of data. Among the policy choices recommended by
14 these Principles in the context of supply or sharing of data is the default position that data supplied
15 may be used by the recipient for any lawful purpose that does not infringe the rights of third parties
16 (‘sales approach’ as opposed to a ‘license approach’). Because, however, the Principles provide a
17 wide berth for private ordering, including provisions that emphasize freedom of contract except
18 when limited by a mandatory rule of the applicable jurisdiction, parties will remain able to agree
19 on arrangements close to a ‘data license’, as is frequently found in model agreements and in data
20 contracts even where data is not protected by intellectual property law.

21 Chapter C deals with contracts whose focus is not the provision of data by one party to
22 another, or the sharing of data among various parties, but rather the provision of services with
23 regard to data. The most important contract type in this regard is contracts for the processing of
24 data, including any cloud storage of data and any data analytics. Another type of contract addressed
25 in Chapter C is a type that has been labeled, for lack of a better term, ‘data trust contracts’, although
26 that term should not be taken as encompassing the specific legal implications of the common law
27 concept of trusts, and a related type of contract labeled ‘data escrow contracts’. Also, data
28 marketplace contracts, which are essentially about the facilitation of data transactions and the
29 matchmaking between parties, are dealt with under this Part.

30 *c. Part III: Data Rights.* The third Part of the Principles is devoted to data rights. It is
31 important to note that Part III goes beyond the type of relationships addressed in Part II. Much of

1 the data economy is not about ‘pure data commerce’, such as a data broker selling data to an ad
2 agency, but about very traditional value chains, involving, e.g., suppliers of components,
3 producers, wholesalers, retailers and end users, with data being generated at various links in that
4 chain. Where parties in that value chain make arrangements about data, e.g., the producer allows
5 the supplier of a component to access data relating to the performance of that component in the
6 producer’s cloud, this is then a contract within the meaning of Part II (e.g., a contract for access to
7 data under Principle 8). In practice, however, parties have often not made proper arrangements
8 concerning such data, which is why Principles are required for outlining to what extent notions of
9 fundamental fairness dictate that such arrangements be made. Typical data rights are access and
10 porting rights, as well as rights to request desistance from a particular data use, correction of data,
11 or even a share in proceeds from data activities. Like the previous Part, Part III starts with a Chapter
12 A on general provisions relevant to data rights.

13 Chapter B of Part III identifies, analyses and collates existing and potential future rules on
14 data rights with regard to what these Principles call ‘co-generated data’. The fact that a party had
15 a share in the generation of certain data—such as by being the subject of the information coded in
16 the data, or owning the device by which data has been generated, or having designed the device
17 with the help of which data is generated—may, together with other factors, give rise to a special
18 relationship between that party and any controller of the data. For example, an important part of
19 the data economy is the supply of goods, digital content (such as software), and services to
20 customers where, through the use of these commodities by the customers or other users, data is
21 generated, and transmitted to and ultimately processed by the supplier or producer of the
22 commodity or any other third party chosen by the supplier or the producer. The Principles analyze,
23 inter alia, the situation of customers with regard to user-generated data, addressing intricate legal
24 issues such as a customer’s access and porting rights, e.g. where the customer wishes to re-sell the
25 commodity or to switch the supplier, as well as other typical constellations in data value chains.

26 While these Principles do not intend to engage in the scholarly debate between ‘privacy
27 theories’ and ‘property theories’ it ought to be noted that the ‘co-generated data’ approach, which
28 has been developed by these Principles and is gaining recognition worldwide, transcends the
29 debate. It does so by combining elements of both theories in a scheme of fairness rules that has
30 been developed specifically with a view to the characteristics of data as a non-rivalrous, multi-
31 functional and extremely dynamic resource.

1 Chapter C on other data rights is on data rights that are afforded to a party without regard
2 to any share the party may have had in the generation of the data. Such rights are typically afforded
3 for public interest purposes, including for the purpose of ensuring fair and undistorted competition
4 and the purpose to make data openly available in order to foster general innovation and growth.
5 Given the broad variety of these data rights, Chapter C can only state some very general Principles,
6 such as concerning proportionality, fairness, non-discrimination and reciprocity.

7 *d. Part IV: Third-Party Aspects of Data Activities.* Part IV deals with third-party aspects of
8 the data activities addressed under the preceding Parts of the Principles. While, e.g., supply or
9 sharing of data are, primarily, about a transaction between two or more parties and about the
10 contractual rights and remedies these parties may have against each other, there are also third
11 parties who may be affected by the transaction and who may have a word to say. This may be the
12 case, e.g., where the onward transfer of data interferes with a right of another party, such as an
13 intellectual property right or a right flowing from data privacy/data protection law.

14 Chapter A sets out general considerations about when data activities are wrongful vis-à-vis
15 protected parties, including situations where data activities fail to comply with contractual
16 limitations, or where access to data has been obtained by unauthorized means.

17 Onward supply of data by a controller may affect such protected parties. Amongst others,
18 clarity must be achieved as to whether and to what extent contractual protection against certain
19 downstream data activities is possible, and what is the effect as against downstream recipients. The
20 Principles suggest, in Chapter B of Part IV, that contractual limitations on data activities may have
21 downstream third party effects under a tort-like regime inspired by trade secrets law, and the same
22 would apply where data had originally been obtained by unauthorized means before being passed
23 on. In suggesting this regime, the Principles seek to strike a balance between the desire to ensure
24 strong protection of existing rights on the one hand and the desire to encourage data sharing and
25 create an economy-friendly environment on the other. Chapter B also deals with the general due
26 diligence duties of parties that pass data on to downstream recipients and with possibilities to take
27 direct action against downstream recipients.

28 Chapter C of Part IV addresses the situation that data has been aggregated with other data,
29 or has otherwise been processed so as to obtain derived data. Clarity needs to be achieved as to
30 whether limitations following from third party rights with regard to the original data set still apply
31 with regard to the derived data set, what are the legal consequences if the answer is yes, and whether

1 any legal consequences with regard to the derived data set follow from the mere fact that the data
2 set has been derived by way of wrongful processing activities.

3 *e. Part V: Multi-State Issues.* Transactions and other activities in the data economy will, by
4 their very nature, hardly ever occur within the confines of national borders. Accordingly, the last
5 Part, without purporting to provide a complete set of choice of law or similar rules, provide some
6 guidance as to the application of rules and doctrines of private international law to issues in the
7 data economy.

1 **PRINCIPLES FOR A DATA ECONOMY**
2 **– DATA TRANSACTIONS AND DATA RIGHTS –**
3 **ELI Final Council Draft**

4 **Part I: General Provisions**

5 **Principle 1: Purpose of these Principles**

6 **(1) The Principles for a Data Economy are intended for use in legal systems in Europe, the**
7 **United States, and elsewhere. They are designed to**

8 **(a) bring coherence to, and move toward harmonization of, existing law and legal**
9 **concepts relevant for the data economy;**

10 **(b) be used as a source to inspire and guide the further development of the law by courts**
11 **and legislators worldwide;**

12 **(c) inform the development of best practices and guide the development of emerging**
13 **standards, including standards or trade codes that are specific to a particular**
14 **industry or industry sector;**

15 **(d) facilitate the drafting of model agreements or provisions to be used on a voluntary**
16 **basis by parties in the data economy;**

17 **(e) govern contracts or complement the law that governs them to the extent that they**
18 **provide default rules or that parties to a transaction have incorporated them into**
19 **their contract or have otherwise designated them to govern; and**

20 **(f) guide the deliberations of tribunals in arbitration and other dispute resolution**
21 **forums.**

22 **(2) These Principles recommend a legal framework that is intended to work with any form**
23 **of data privacy or data protection law, intellectual property law, or trade secrets law.**
24 **These Principles are not intended to amend or create any such law, but they may inform**
25 **the development of such other law. In the event of any inconsistency between these**

1 **Principles and such other law that cannot be overcome by interpretation, the other law**
2 **should prevail.**

3 *Comment: a. Addressees and added value.* These Principles address a fast-emerging but
4 already major sector of the economy. Yet, this sector has developed largely without a legal
5 framework that recognizes and reflects many of the sector’s important and unique attributes in
6 order to govern it in a way that thoughtfully balances and facilitates both the public interest and the
7 private interests of the parties. These Principles are the result of collaborative work of lawyers from
8 Europe and the U.S. They are designed to provide guidance as to the basic principles to be applied
9 to data transactions and related matters irrespective of the otherwise applicable legal framework
10 (whether that of a U.S. state or one of the European legal systems), and thereby seek to develop a
11 consistent, general approach across national borders and legal disciplines.

12 The purpose of these Principles is to provide guidance to and to inform parties, practitioners,
13 arbitral tribunals, standardization bodies, courts, and legislators worldwide. They seek to promote
14 the enhancement and better adaptation of the law to the data economy as an ever more important
15 part of the economy at large and to identify guiding principles in dealing with data as an asset and
16 tradeable item. By doing so, they facilitate the further development of the law by courts and
17 legislators worldwide and the review of existing law and soft law instruments by, in particular,
18 legislative bodies, standardization agencies, or bodies developing codes of conduct. The Principles
19 are also designed to facilitate the drafting of model agreements or provisions to be used on a
20 voluntary basis by parties in the data economy. Equally, they may govern contracts or
21 complement the law that governs contracts to the extent that they provide default rules or that
22 parties to a transaction have incorporated them into their contract or have otherwise designated
23 them to govern. The Principles may, in a similar vein, guide the deliberations of tribunals in
24 arbitration and other dispute resolution forums (such as mediation). Depending on the specific
25 needs and characteristics of a particular industry these Principles may provide the basis for
26 adaptation or extension for the development of industry-specific standards.

27 By their very nature, some Parts of these Principles are addressed to particular players more
28 than to others. For instance, Part II on data transactions is addressed both to parties in the data
29 economy (and to counsel advising these parties), bringing some clarity as to the main types of
30 transactions and suggesting rules that could typically be considered reasonable and fair, and to
31 courts, which must deal with incomplete agreements and provide appropriate ‘gap fillers’ when

1 parties have failed to deal with important issues. Part III on Data Rights is predominantly addressed
2 to legislators and bodies developing standards and codes of conduct. However, it is also addressed
3 to parties, their legal advisers, and to courts dealing with issues that involve the relationship
4 between, e.g., the users of goods, digital content or services and the manufacturer, or between the
5 manufacturer and suppliers of components. Part IV may be seen to be addressed primarily to
6 legislators considering issues raised by the data economy, and to courts that have been called upon
7 by a party, e.g., because that party claims its rights have been infringed by some data activity. The
8 same would hold true for Part V dealing with cross-border issues. However, none of the Parts is
9 exclusively targeted at the specific audiences just mentioned, and these Principles seek to provide
10 added value to as broad a variety of actors as possible.

11 *b. Relationship with specific areas of the law not addressed by these Principles.* The data
12 economy is a subject that touches upon and cuts across many areas of the law. Most notably, data
13 may in many instances be protected by copyright or other intellectual property rights. In addition,
14 to the extent that data is personal data (i.e. is identified, or identifiable, to a particular natural
15 person), data privacy/data protection law provides for an ever more comprehensive set of rules.
16 Another area of the law with a firmly established framework that addresses the protection of
17 information and data is trade secret law. While these Principles cannot entirely avoid referring to
18 these areas of the law, they do not seek to restate what the rules in those areas are or should be.
19 Rather, they take those areas of the law as more or less given.

20 For example, these Principles propose rules to govern transactions in non-personal data as
21 well as personal data, recognizing that the latter type of data may be subject to data privacy/data
22 protection regimes. The Principles, in some cases, address some implications of such regimes for
23 trade in data. But the Principles do not deal with issues fully covered by data privacy/data protection
24 law, such as when consent is necessary and/or can be withdrawn.

25 **Illustration:**

26 1. Business S supplies an online video game and holds a broad range of personal data
27 from users playing that game, much of which is protected under data privacy regimes
28 such as the California Consumer Privacy Act (CCPA) or the General Data Protection
29 Regulation (GDPR). S ‘sells’ the data of 20,000 users to data analytics business R in a
30 way that is in conformity with the relevant data privacy regimes. Shortly after the data

1 is transferred to B, 5,000 users from the EU withdraw their consent to the processing of
2 the data. As a reaction, R demands return of 25% of the price paid to S. As these
3 Principles do not seek to restate or revise data privacy/data protection law, they do not
4 deal with questions such as whether the users' consent may be withdrawn at any time,
5 or whether the users have a right to object to the sale by clicking a button stating 'Do
6 not sell my data' or the like. Rather, user rights under data privacy/data protection law
7 are left to the applicable rules, considering also the territorial scope of those rules. The
8 Principles do, however, address the effect of data privacy/data protection regimes, and
9 of rights exercised under such regimes, on the rights of parties to a data transaction such
10 as the transaction between S and B, e.g., whether S would have been under a duty to
11 make R aware of this risk and whether R has any rights against S because R ultimately
12 lost 25% of what R had bargained for.

13 Sometimes, the validity of a transaction dealt with under these Principles will depend on
14 such other law, e.g., where a transaction is blatantly inconsistent with data privacy/data protection
15 law that may, depending on the circumstances, mean the transaction is illegal and thus void or
16 voidable under the applicable law. That, too, is not a matter for these Principles to deal with.

17 **Illustration:**

18 2. Assuming that, in a scenario such as that in Illustration 1, a large number of users had
19 failed to give their consent, or had really clicked the button 'Do not sell my data', and
20 thus 'sale' and transfer of the data by S to R was really against the law, and both S and
21 R were aware of that. Whether that affects in any way the validity of the contract
22 between S and R should not be for these Principles to deal with. However, these
23 Principles will then deal with what the unwinding of the transaction means with regard
24 to the data.

25 Sometimes, different aspects of the same activity may be the subject of these Principles as
26 well as other bodies of law. For instance, data porting (portability) rights are dealt with under Part
27 III of these Principles, but they may also be an element of data protection law, consumer protection
28 law, or competition law. It is, in particular, in those grey zones that the other bodies of law would
29 prevail in the event of any inescapable inconsistency between them and these Principles, but still
30 these Principles might inform the development of these other bodies of law and point at directions

1 of development that might be more favorable for a flourishing data economy than others. For
2 example, a major challenge for the data economy is that there is hardly any data pool that does not
3 implicate potential issues arising from data privacy/protection law (e.g. because some data in the
4 pool is personal data, or can be de-anonymized in the future), intellectual property law (e.g. because
5 some snippets of text might be protected by copyright) or trade secrets law (e.g. because aggregated
6 machine data allow conclusions about business operations). This leads to reluctance on the part of
7 businesses to share their data with others as such sharing might indirectly expose them to requests
8 for erasure, claims for damages and other adverse consequences. The law should take these
9 considerations into account when accommodating these diverse needs, and Principles 34, 36 and
10 37 in particular make some suggestions as to how this could be achieved.

11 *c. Relationship with contract rules and doctrines.* The relationship of the data economy
12 Principles to existing law of sales and service contracts, such as can be found in European civil
13 codes or statutes or in the Uniform Commercial Code, is an entirely different story. There is a clear
14 overlap between such areas of the law and these Principles, such as with regard to contractual rights
15 and obligations of the parties. These Principles are inspired by those bodies of law and are guided
16 by them, sometimes clarifying application of existing principles in the data context while other
17 times providing a roadmap for future development. They seek to identify standards that, if adopted,
18 would take priority over existing rules in these areas by tailoring their application to data
19 transactions. The same holds true for unfair competition law, which, however, normally does not
20 specifically deal with data or information and would be informed by these Principles only with
21 regard to data economy scenarios.

22 These Principles do not address general legal doctrines such as those governing formation
23 of contracts or protections provided to consumers in consumer contracts, leaving those matters to
24 existing law. Thus, these Principles do not differentiate between consumers and businesses as
25 customers. Rather than create new protective doctrines unique to this context, these Principles
26 instead provide guidance as to the application in a data setting of existing protective rules and
27 doctrines, which often differentiate between consumers and businesses. Whenever these Principles
28 refer to ‘contract’ or ‘contractual’ this automatically implies that all general contract law doctrines,
29 whether from statute or common law, apply, and that, where the contracting parties are a business
30 and a consumer, all applicable consumer protection standards remain unaffected. These doctrines
31 and standards vary from jurisdiction to jurisdiction (e.g. notions of ‘unconscionably’ and

1 ‘unfairness’ in business-to-business transactions may mean very different things in different
2 jurisdictions), and it is not the purpose of these Principles to change, with regard to data, a more
3 general approach taken by the contract law of a particular jurisdiction on these matters.

4 *d. Relationship with property law.* These Principles do not address whether rights in data
5 are to be characterised as ‘ownership’ or ‘property’ (except, of course, when other law, such as
6 intellectual property law or the like, affirmatively creates property rights), nor do they take any
7 position in the controversy between more privacy-oriented and more property-oriented theories of
8 data law. Rather, they describe the attributes of rights with regard to data without addressing the
9 issue of ‘proper’ doctrinal characterisation as the one or the other.

10 REPORTERS’ NOTES

11 U.S.:

12 Principle 1(1) is based on the structure of a number of “soft law” instruments. See, e.g.,
13 UNIDROIT Principles of International Commercial Contracts, Preamble (2016); Hague Principles
14 on Choice of Law in International Commercial Contracts, Preamble (2015).

15 U.S. bodies of law that apply to matters also addressed in these Principles include most
16 particularly contract law (see Restatement of the Law, Second, Contracts (1980)) and tort law (see
17 Restatement of the Law, Third, Torts: Liability for Economic Harm (2020)). Contract law
18 principles in Article 2 of the Uniform Commercial Code do not apply directly to data transactions
19 (because data does not constitute “goods” (see UCC §§ 2-102, 2-105)), but can be a source of
20 useful analogies. Principles that address security interests in data are also governed in the U.S. by
21 Article 9 of the Uniform Commercial Code.

22 U.S. bodies of law that can apply to data transactions, and to which these Principles defer,
23 include data privacy law (see Principles of Law, Data Privacy), copyright law (see Restatement of
24 the Law, Copyright (pending)), and property law (see Restatement of the Law Fourth, Property
25 (pending)).

26 For a thoughtful analysis of the need for special contract law for data transfers, see Kevin
27 E. Davis and Florencia Marotta-Wurgler, Contracting for Personal Data, 94 N.Y.U. L. Rev. 662
28 (2019). For an analysis of establishing principles for data by analogy to other subjects, see Lauren
29 Henry Scholz, Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies,
30 available at SSRN: <https://ssrn.com/abstract=3252543> or <http://dx.doi.org/10.2139/ssrn.3252543>.

31 In the U.S., see and compare paragraph (1) with, e.g., UCC § 1-103, which identifies
32 underlying purposes and policies of the Uniform Commercial Code as (i) simplification,
33 clarification, and modernization of the law governing commercial transactions, (ii) permitting the
34 continued expansion of commercial practices through custom, usage, and agreement of the parties,
35 and (iii) making uniform the law among various jurisdictions. As stated in Official Comment 1 to
36 UCC § 1-103, “The Uniform Commercial Code should be construed in accordance with its
37 underlying purposes and policies. The text of each section should be read in light of the purpose
38 and policy of the rule or principle in question, as also of the Uniform Commercial Code as a whole,

1 and the application of language should be construed narrowly or broadly, as the case may be, in
2 conformity with the purposes and policies involved.”

3 As to whether rights in data are to be characterised as “ownership” or “property,” the
4 literature is extensive. See, e.g, Lothar Determann, *No One Owns Data*, 70 *Hastings L.J.* 1 (2018)
5 (“The rationales for propertizing data are thus not compelling and are outweighed by the rationales
6 for keeping the data ‘open.’ No new property rights need to be created for data.”); Margaret Jane
7 Radin, *A Comment on Information Propertization and Its Legal Milieu*, 54 *C. S. L. R.* 23, 25 (2006)
8 (noting that “Propertization of information not included in copyright has been significantly
9 expanded through resurrection of a metamorphosed version of the common-law doctrine of trespass
10 to chattels”); Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing*
11 *Property in Databases*, 18 *B. T. L.J.* 773, 787 (2003).

12 Of course, even discussing whether rights in data are to be characterized as property rights
13 presupposes a common concept of what constitutes “property.” Scholarship of the last few decades
14 makes it clear that law has not settled on such a concept and, moreover, that the concept can have
15 different meanings in different contexts. But “property is an artifact, a human creation that can be,
16 and has been, modified in accordance with human needs and values.” Hanoch Dagan, *The Craft of*
17 *Property*, 91 *C. L. R.* 1518, 1532 (2003).

18 For an extensive discussion of the nature of “property” and “ownership” in general, see
19 *Restatement of the Law, Fourth, Property* (Council Draft No. 1 2019) §§ 1-3.

20 **Europe:**

21 *a. Addressees and added value.* As already pointed out in the US Notes, the structure of
22 Principle 1(1) draws inspiration from internationally well-recognized ‘soft law’ instruments such
23 as Article 1:101 of the Principles of European Contract Law (PECL), the Preamble of the
24 UNIDROIT Principles of International Commercial Contracts (2016) or of the Introduction to the
25 Hague Principles on Choice of Law in International Commercial Contracts (2015).

26 Paragraph (1) clarifies the Principles’ intent to be sufficiently concrete to allow for the
27 solution of a variety of legal problems ‘on the ground’ and provide guidance for a broad variety of
28 actors. Existing standards and frameworks have been an essential source of inspiration for these
29 Principles. However, frameworks with a similarly broad scope, such as the UN Global Pulse
30 Principles (United Nations Development Group, ‘Data Privacy, Ethics and Protection Guidance
31 Note on Big Data for Achievement of the 2030 Agenda’, 2017), the OECD Principles (OECD,
32 *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across*
33 *Societies*, 2019, p. 12), the Principles formulated by the Danish Data Ethics Council (The Expert
34 Group on Data Ethics, ‘Data for the Benefit of the People’, 2018, p. 34), and the German Data
35 Ethics Commission (Opinion of the Data Ethics Commission, 2019, p. 6 f.), as well as the principles
36 put forward by the Finnish EU Presidency (Finland’s Presidency of the Council of the European
37 Union, *Principles for a human-centric, thriving and balanced data economy*, 2019), are on a higher
38 level of abstraction and of a more aspirational nature, compared to these Principles.

39 More concrete are the ‘data strategies’ that have been presented e.g. by the European
40 Commission (COM(2020) 66 final) and certain European states (e.g. Data Strategy of the United
41 Kingdom, 2020; Data Strategy of the German Federal Government, *Datenstrategie der*
42 *Bundesregierung*, 2021). Some states did not address their intentions to introduce comprehensive
43 legal frameworks for the data economy in genuine ‘data strategies’ but implemented them in their
44 strategies on Artificial Intelligence (see the French AI Strategy: Villani Report, 2018, p. 20 ff).
45 These strategies already formulate legislative measures that should be enacted in the future and

1 thus provide an outlook on the possible legal landscape of the near future. However, they limit
2 themselves to this outlook and do not yet contain any material proposals for legal acts.

3 Concrete guidance to parties who have decided to enter into a ‘data transaction’ is achieved
4 by the handful of existing model agreements for data transactions (see the ‘Report on collected
5 model contract terms’ by the Support Centre for Data Sharing; the Dutch vision on data sharing
6 between businesses by the Dutch Ministry of Economic Affairs, or the ‘Danish model agreements
7 for data transfers’). The most advanced initiative seems to be the ‘Contract Guidelines on
8 Utilization of AI and Data – Data Section’ published by the Japanese Ministry of Economy, Trade
9 and Industry (METI) (METI, Contract Guidelines on Utilization of AI and Data – Data Section,
10 2018). However, model agreements cannot give guidance to courts or legislators as to whether
11 parties must enter into negotiations about a transaction, pay damages to each other, etc. Compared
12 to the listed principles, standards and strategies, the Principles have a more comprehensive scope,
13 as, on the one hand, they target various audiences, and on the other aim to address a variety of
14 different legal problems on a level of concreteness that allows solving legal problems ‘on the
15 ground’. They can further serve as guidance, for future legislative measures announced in the data
16 strategies, e.g. for the Data Act (2021).

17 *b. Relationship with specific areas of the law not addressed by these Principles.* The EU
18 has introduced several instruments that – either directly or indirectly – produce effects for the data
19 economy, and thus also affect the subject matter of these Principles. Areas of law where such
20 instruments exist include data privacy/data protection law, copyright or other intellectual property
21 law, and trade secret law.

22 As far as personal data is concerned, it is in particular the General Data Protection
23 Regulation (GDPR, Regulation (EU) 2016/679) that regulates the lawfulness of processing of
24 personal data and data subjects’ rights. In addition, the E-Privacy Directive (Directive 2002/58/EC)
25 lays down rules for the processing of personal data in the electronic communication sector. The
26 latter should already have been replaced by a new Regulation some years ago (cf. Commission
27 Proposal COM(2017), 10 final), but the Council only recently agreed on a first common position
28 after the proposal had been stuck for years in negotiations.

29 In the field of intellectual property there are numerous instruments on an EU level that may
30 also cover data. Of particular relevance for the data economy are the Database Directive (Directive
31 96/9/EC), the Information Society Services Directive (Directive 2001/29/EC) and the Copyright
32 DSM Directive (Directive (EU) 2019/790). But data may also be covered by more specific regimes,
33 such as the Software Directive (Directive 2009/24/EC). Finally, data are protected under the Trade
34 Secrets Directive (Directive (EU) 2016/943) against unlawful acquisition, use and disclosure.

35 *c. Relationship with contract rules and doctrines.* The relationship between provisions of
36 European civil codes that have inspired and guided these Principles, or that serve as the basis for
37 analogies, are discussed at length in the Notes to the Principles of Part II. Basic contract law
38 doctrines, such as on the formation, nullity and validity of a contract, are not only excluded by the
39 Principles, but are left to national law even by comprehensive EU contract law regimes. Even the
40 Digital Content and Services Directive (DCSD, Directive (EU) 2019/770), which is by far the most
41 advanced European Act on data contracts, leaves this issue to the applicable national law (see
42 Article 3(10) DCSD).

43 *d. Relationship with property law.* Whether to introduce a ‘data ownership’ right was the
44 subject of intensive debate from a policy point of view. While the European Commission
45 considered introducing a ‘data producer’s right’ at EU level in its Communication on ‘Building a
46 European Data Economy’ (COM(2017) 9 final, p. 10 ff), it changed its position after severe
47 criticism that the introduction of such a new intellectual property right could be detrimental to the

1 data economy. Currently, the predominant view in Europe seems to be that access rights and similar
2 data rights are more promising as a way forward than data ownership rights (COM(2020) 66 final
3 p. 4 ff.; COM(2018) 232 final, p. 9). For more detailed elaborations, see Reporters' Notes to
4 Principle 16.

5 **Principle 2: Scope of these Principles**

6 **(1) The primary focus of the Principles is on records of large quantities of information as**
7 **an asset, resource or tradeable commodity. The Principles do not address functional**
8 **data, i.e. data the main purpose of which is to deliver particular functionalities (such as**
9 **a computer program), and representative data, i.e. data the main purpose of which is to**
10 **represent other assets or value (such as crypto-assets).**

11 **(2) Subject to paragraph 3, these Principles address**

12 **(a) data contracts,**

13 **(b) data rights, and**

14 **(c) third party aspects of points (a) and (b).**

15 **(3) These Principles are not designed to apply to public bodies insofar as such bodies are**
16 **engaging in the exercise of sovereign powers.**

17 **Comment:** *a. Focus on information.* The definition of 'data' in Principle 3(1)(a) is broad.
18 Applying the Principles to all rights and transactions about data (as so defined) would result in
19 application of the Principles beyond their intended context. The Principles (as well as the terms
20 'data contracts', 'data rights' etc.) should be understood as covering only issues that have a primary
21 focus on records of large quantities of information. They should not cover cases where, e.g., the
22 focus is on the medium itself, or on an entirely different aspect of data. This flexible approach
23 allows for these Principles to be applied to the whole transaction, to a particular part or aspect of a
24 transaction, or not applied at all when the 'records of information' aspect is not the focus of the
25 subject matter.

26 **Illustrations:**

27 3. A simple contract between a law firm and a client pursuant to which the law firm will
28 represent the client in contract negotiations would not be within the scope of the

1 Principles even where it is anticipated that the law firm will transmit proposed drafts of
2 transactional documents in digital form through an electronic message system. This is
3 because the focus of the contract between the law firm and the client is not on the
4 records of information, but rather the legal advice as such. Of course, a wider
5 relationship between a law firm and a client may include aspects that are within the
6 scope of these Principles, and that relationship may include, e.g., access to data or
7 processing of data within the meaning of the Principles.

8 The distinction between a primary focus on records of (large quantities of) information and
9 a different focus is particularly relevant when it comes to digital phenomena that are not primarily
10 considered as ‘data’ even though, technically speaking, they have the same or a very similar nature.
11 A computer program, for example, is primarily seen as a set of commands delivering particular
12 functionalities (‘functional data’). Cryptocurrencies and other tokens may be seen as, amongst
13 others, data packets, but clearly the focus is not on any value inherent in the information recorded
14 in the token, but rather on the off-ledger asset represented by them (‘representative data’) or the
15 on-ledger asset generated by the fact that other members of a community are prepared to trade them
16 for value. This is why Principle 2(1) clarifies that the Principles do not address functional data or
17 representative data.

18 **Illustrations:**

19 4. A transfer of Bitcoins from wallet holder A to wallet holder B is not a ‘data transaction’
20 for purposes of these Principles because the transaction is primarily about a transfer of
21 value represented by a virtual token and documented on the blockchain. Likewise, in-
22 game purchase of a weapon or superpower would not be a ‘data transaction’ and would
23 not be covered by the Principles because the focus is on the functionality, not on the
24 information.

25 The fact that a set of digital data normally serves the purpose of delivering certain
26 functionalities does not exclude the possibility that the same set of data may also be used without
27 reference to those functionalities, in which case the data could be within the scope of these
28 Principles.

1 *b. Asset, resource or tradeable commodity.* Information has always been subject to a variety
2 of different contracts, in particular service contracts, and information rights have always been
3 included in a wide range of different legal regimes. Many of these issues fall outside the scope of
4 the Principles already because they are not about ‘digital’ data, or because the information is not
5 the focus of the transaction. However, there are cases where the law provides that, e.g., particular
6 information must be given to a consumer with particular digital means, or where two parties agree
7 in a contract that one party will disclose and publish all its conflicts of interest on the party’s
8 website. In these cases, the legal rules are about digital data, and they are about the information
9 aspect, but still such rules would not be within the focus of these Principles. This is because these
10 Principles are not primarily concerned with single pieces of information provided with the aim of
11 immediately letting another party *know* something, but more about ‘bulk’ or ‘serial’ data, usually
12 to be processed with the help of machines, and used as an asset, resource or tradeable commodity.
13 Accordingly, supplying data within the meaning of these Principles is not so much about *doing*
14 something, but more about *delivering* something.

15 *c. Issues addressed.* The development and identification of clear and certain principles
16 which promote a data economy that is both efficient and fair is of fundamental importance to the
17 development of that economy. Law governs the data economy in a wide variety of ways. These
18 include the allocation of private rights with respect to transactions and the data to which the
19 transactions relate, unfair competition and antitrust law, privacy and data protection law, etc. These
20 Principles do not address that entire range of legal issues but, rather, focus on data contracts and
21 data rights, and on the third-party aspects of such contracts and rights, as far as these are relevant
22 in the context. In addition, the Principles provide some limited guidance as to multi-state issues
23 with regard to data contracts and data rights, without providing a full set of choice-of-law rules.

24 *d. Public bodies.* The control and processing of data by public bodies in the exercise of
25 sovereign powers afforded to them by the applicable law is an extremely important topic which is,
26 however, beyond the boundaries of these Principles. The Principles therefore apply only to the
27 extent that exercise of sovereign powers is not implicated (but even where the Principles could be
28 applied to activities of public bodies, other, more specific, rules for dealings with the government
29 or government agencies may also apply).

Europe:

1
2 *a. Focus on information.* The explicit reference to the focus on information in the scope of
3 the Principles is unique from a European point of view. The same holds true for the terms
4 ‘representative data’ and ‘functional data’ in paragraph (1), which are not defined at EU level.
5 However, since the term ‘representative data’ also covers crypto-assets, there are certain overlaps
6 with existing definitions of virtual currencies, which are defined as ‘a digital representation of value
7 that is not issued or guaranteed by a central bank or a public authority’ (see Article 1(2)(d) of
8 Directive (EU) 2018/843). The term ‘functional data’ reflects the basic understanding in software
9 engineering that a distinction must be made between the binary code of a computer program and
10 other or ‘mere’ data. The digital data that make up a computer program are characterized by the
11 property that they enable computer hardware to perform computational or control functions (see
12 IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990). That
13 computer programs perform a control function is also recognized by EU law (see recital 10 of
14 Directive 2009/24/EC).

15 Even though the explicit scope of the Principles is unique, it is clear from the subject matter
16 that some legislations (implicitly) have the same focus. This is true for the Data Governance Act
17 (DGA, COM(2020) 767 final), which wants to improve the conditions for data sharing in the
18 internal market and, e.g., lays down a notification and supervisory framework for the provision of
19 data sharing services (Articles 9 ff DGA). However, ‘functional’ and ‘representative data’ – as
20 used in paragraph (1) – are not explicitly excluded from its scope of application. And the definition
21 of data as ‘digital representation of acts, facts or information and any compilation of such acts,
22 facts or information, including in the form of sound, visual or audiovisual recording’ (Article 2(1)
23 DGA), may be too broad to ensure that the DGA does not apply to data that does not have a primary
24 focus on information. It can, for example, be argued that a bitcoin is the digital representation of
25 facts and information, namely the value, time and recipient of a transaction.

26 The broad definition of ‘digital content’ in Article 2(1) Digital Content and Services
27 Directive (DCSD, Directive (EU) 2019/770) covers functional data within the meaning of
28 paragraph (1) as well as digital data where the primary focus is on records of large quantities of
29 information as an asset, resource or tradeable commodity. However, contrary to the Principles, the
30 primary focus of the Directive is not on information, but on the functional level of data. Digital
31 representations of value such as electronic vouchers, e-coupons or cryptocurrencies, i.e.
32 representative data, are also explicitly not covered by the Digital Content and Services Directive
33 (Recital 23 DCSD).

34 *b. Asset, resource or tradeable commodity.* EU instruments are typically not limited to large
35 quantities of data with a primary focus on information. The GDPR, for example, applies to the
36 processing of personal data, which Article 4(1) defines ‘as any information relating to an identified
37 or identifiable natural person’. The Free Flow of Data Regulation refers to Article 4(1) GDPR to
38 define non-personal data and thus does not exclude single pieces of information provided with the
39 aim of immediately letting another party know something.

40 *d. Public bodies.* European legislations on data oftentimes exclude *public bodies acting* in
41 the exercise of their sovereign powers from the scope of application and *vice versa*. For example,
42 the Open Data Directive (Directive (EU) 2019/1024) is addressed to public bodies, and excludes
43 documents, the supply of which is an activity falling outside the scope of the public task of the
44 public sector bodies concerned, from the scope of application (Article 1(2)(a) Open Data
45 Directive). It is in a similar vein, that Principle 2(3) does not apply to public bodies insofar as such
46 bodies are engaging in the exercise of sovereign powers. For guidance as how to interpret Principle
47 2(3), see Article 1 of the Brussels Ia Regulation (Regulation (EU) No 1215/2012), which contains

1 a similar public-private law division and only applies where the public authority acts in the exercise
2 of its public powers (CJEU Case C-645/11 para 33 – *Sapir et al*).

3 **Principle 3: Definitions¹**

4 **(1) For the purposes of these Principles the following definitions shall apply:**

5 **(a) ‘Data’ means information recorded in any machine-readable format suitable for**
6 **automated processing, stored in any medium or as it is being transmitted;**

7 **(b) ‘Copy’ means any physical manifestation of data in any form or medium;**

8 **(c) ‘Processing data’ means any operation or set of operations that is performed on**
9 **data, whether or not by automated means; it includes, inter alia, the structuring,**
10 **alteration, storage, retrieval, transmission, combination, aggregation or erasure of**
11 **data;**

12 **(d) ‘Access to data’ means being in a position to read the data and utilize it, with or**
13 **without having control of that data;**

14 **(e) ‘Control of data’ means being in a position to access the data and determine the**
15 **purposes and means of its processing;**

16 **(f) ‘Controller’ means the person that, alone or jointly with other persons, has control**
17 **of data;**

18 **(g) ‘Processor’ means a person that, without being a controller, processes data on a**
19 **controller’s behalf;**

20 **(h) ‘Co-generated data’ means data to the generation of which a person other than the**
21 **controller has contributed, such as by being the subject of the information or the**
22 **owner or operator of that subject, by pursuing a data-generating activity or owning**

¹ These definitions follow the tradition in many international legal texts of placing definitions in the order in which the defined terms appear in the text. The comments, which explain and elaborate on these definitions, appear in groups of related terms. We understand that many readers, particularly in the U.S., would prefer that the definitions, and their accompanying comments, appear in alphabetical order; accordingly we are considering that change and seek input from the Councils and Membership of both ALI and ELI. Any decision should consider that these Principles might be translated into other languages, particularly in Europe.

- 1 **or operating a data-generating device, or by producing or developing a data-**
2 **generating product or service;**
- 3 **(i) ‘Derived data’ means data generated by processing other data and includes**
4 **aggregated data and data inferred from other data with the help of external decision**
5 **rules;**
- 6 **(j) ‘Data contract’ means a contract the subject of which is data;**
- 7 **(k) ‘Data right’ means a right against a controller of data that is specific to the nature**
8 **of data and that arises from the way the data is generated, or from the law for**
9 **reasons of public interest;**
- 10 **(l) ‘Data activities’ means activities by a person with respect to data, such as collection,**
11 **acquisition, control, processing and other activities including onward supply of**
12 **data;**
- 13 **(m) ‘Supply’ of data means providing access to data to another person or putting**
14 **another person in control of data;**
- 15 **(n) ‘Supplier’ of data means a party who supplies data to another party, or undertakes**
16 **to do so;**
- 17 **(o) ‘Recipient’ of data means a party to whom data is supplied, or to be supplied;**
- 18 **(p) ‘Transfer’ of data means supply of data by way of which the supplier puts the**
19 **recipient in control of the data, whether or not the supplier retains control of the**
20 **data;**
- 21 **(q) ‘Porting’ data means initiating the transfer of data controlled by another party to**
22 **oneself or to a designated third party;**
- 23 **(r) ‘Erasure of data’ means taking steps to assure, as far as is reasonably possible, that**
24 **the data is permanently inaccessible or otherwise unreadable; and**
- 25 **(s) ‘Notice’ means having knowledge of a fact or, from all the facts and circumstances**
26 **of which a person has knowledge, being in a position that the person can reasonably**
27 **be expected to have known of the fact.**

- 1 **(2) The terms ‘contract for the transfer of data’, ‘contract for simple access to data,**
2 **‘contract for exploitation of a data source’, ‘contract for authorization to access’,**
3 **‘contract for data pooling’, ‘contract for the processing of data’, ‘data trust contract’,**
4 **‘data escrow contract’ and ‘data marketplace contract’, and any terms denoting the**
5 **parties to such contracts, have the meanings given to them in Principles 7 to 15.**
- 6 **(3) References to a ‘person’ include natural and legal persons, private or public. References**
7 **to an ‘operation’ or ‘activity’ shall include operations or activities carried out with the**
8 **help of other persons or of machines, including any artificial intelligence.**

9 **Comment:** *a. ‘Data’ and ‘copy’.* These Principles are concerned only with data that is in a
10 machine-readable format suitable for automated processing. In common parlance, such data is often
11 referred to as ‘digital’ data. However, these Principles are intended to cover also non-digital
12 technologies (such as analog computing and, perhaps, quantum computing) when those
13 technologies enable comparable sorts of operations to be performed on the data by automated
14 means, i.e. where data is recorded in other machine-readable formats suitable for automated
15 processing. The intent, however, is to cover only data that is immediately suitable for automated
16 processing by machines, not data can be made suitable for such processing only by means of
17 intervening technologies such as document scanners, or similar technical means.

18 **Illustration:**

- 19 6. Company N runs a news website. N collects a wide range of data concerning the search
20 requests and browsing habits of its visitors and records this data electronically. These
21 Principles address matters with respect to this sort of data.

22 Thus, as used in these Principles, ‘data’ would not cover the content of paper files even
23 though that content can be made suitable for automated processing by way of a scanner and
24 appropriate software. However, these Principles may also be appropriate for application by analogy
25 to other recorded information in some circumstances depending on, inter alia, the way the
26 information is recorded and the manner in which it is to be used.

27 **Illustrations:**

- 28 7. Business B has maintained many years of historical business records, which are
29 recorded on charts printed on paper. Because those charts are not immediately suitable

1 for automated processing, these Principles do not address matters with regard to this
2 sort of data. If, however, the charts were scanned and the resulting data was stored in
3 machine-readable format these Principles would address matters with regard to the data.

4 8. Employee E of business B (unlawfully) ‘sells’ B’s customer database to competitor C.
5 However, due to specific IT security measures taken by B, it turns out to be easier for
6 E to print the customer data on paper to deliver to C than to store the information on a
7 digital medium or transmit it online to C. C will immediately scan the prints and convert
8 the data into a digital format. In a setting like this it would not seem appropriate to
9 restrict the application of these Principles – such as the Principles on unauthorized
10 access and what it means for a downstream recipient – to the phases when the customer
11 data is in digital format. (Note that issues of criminal and other liability on the part of E
12 are beyond the scope of the Principles).

13 The term ‘data’ has multiple facets in common parlance. In fact, lawyers frequently talk
14 past each other when using the term because they are referring to different facets or concepts of
15 ‘data’. Much confusion has been caused, in particular, by the varying use of the terms ‘information’
16 on the one hand and ‘data’ on the other. These Principles use ‘data’ to refer to information recorded
17 in any form or medium, or being in a state of transmission. In the case of digital data, this means
18 that data is more than the binary electrical impulse stored or being transmitted, as it includes context
19 and semantics. Context and semantics are to be found in metadata, domain tables etc.

20 The term ‘data’ as defined in paragraph (1)(a) has more than one layer. For apart from the
21 semantic layer, i.e. the layer that constitutes meaning, it can be understood as referring to the code
22 as such (e.g. a characteristic binary string of ‘0s’ and ‘1s’) or its physical manifestation on a
23 particular medium. The former can be ‘coded’, ‘modified’, ‘decompiled’ etc, while the latter can
24 be ‘stored’, ‘damaged’, ‘erased’ etc. In order to make this distinction more transparent these
25 Principles restrict the term ‘data’ to the former, i.e. to the code as such (including context and
26 semantics), while the physical manifestation on a medium is called a ‘copy’. A term that is often
27 used with a similar meaning is ‘file’, which, however, seems also to have some associations that
28 are not intended in this context.

1 **Illustration:**

2 9. Business B collects data concerning B's transactions with its customers, such as A, on
3 a local hard disk drive, but there is a backup on a cloud server provided by C. The fact
4 that A has bought a specified commodity from B on a specified date is the information.
5 This information is recorded in the form of coded binary impulses, i.e. a characteristic
6 string of '0s' and '1s', which constitutes the data. This string can be found as a physical
7 manifestation both on B's local hard disk drive and on C's cloud server, so there exist
8 two copies of the data (or really even more, as there will be redundancies, and as there
9 may be transitional copies in the cache of several devices).

10 The definition of the term 'copy' applies only as the term is used in these Principles. The
11 definition here is not intended to resolve issues about the meaning of that term in other areas of the
12 law, such as copyright law.

13 *b. 'Processing data' and 'access to data'.* A central term is 'processing' data, which is
14 defined to include any operation or set of operations that is performed on data. Thus 'processing'
15 includes operations such as organising, structuring, storing, adapting or altering, retrieving,
16 transmitting, aligning or combining, restricting, erasing or destroying data. Some of these
17 operations directly target the data as such, while others target the data only indirectly by targeting
18 one or all existing copies. Defining the term generically to cover all of these operations is useful
19 because, given the multitude of different ways in which data can be handled or used, it would be
20 quite unwieldy to utilize different terminology for each of them and, given the pace at which
21 technology is developing, any terminology defined today may be incomplete or inappropriate
22 tomorrow.

23 'Access to data' and processing of data are closely related notions. 'Access' means being
24 in a position to read the data and utilize it, in unspecified or specified ways, and with or without
25 having control of that data. Processing of data usually requires access to the data. Access,
26 conversely, often includes some kind of processing, but not necessarily so; merely reading data on
27 a screen would amount to access but normally not to processing, at least not in the more narrow
28 sense adopted by these Principles.

1 **Illustration:**

2 10. Business B in Illustration no. 9 processes transactional data by structuring them,
3 analyzing them, and by way of many other operations. Assuming B checks its
4 transactions with A because A has filed a complaint (e.g. A claims never to have
5 received a commodity for which he has been billed), retrieving transactional data from
6 either the local drive or the cloud and making it visible on a screen on one of B's devices
7 amounts to processing (and a form of accessing). If B lets A look at the screen and read
8 the information about A's shopping history this is a situation where access (on the part
9 of A) is not accompanied by processing.

10 *c. 'Control of data', 'controller' and 'processor'.* Another central notion is that of 'control
11 of data'. 'Control of data' means being in a position to access the data and to determine the purposes
12 and means of its processing, with or without having a right to do so. A 'controller' means the
13 natural or legal person, public authority, agency or other body that, alone or jointly with others, has
14 control of data.

15 **Illustration:**

16 11. Business B in Illustration no. 9 has its business data stored in cloud space on servers
17 operated by C. B has the access credentials required to access and process the data as B
18 deems appropriate. Even though B is not in 'physical' control of the medium, B has, for
19 the purposes of these Principles, control of the data and qualifies as controller. C does
20 not qualify as a controller insofar as there are features in place, be they of a technical or
21 legal nature, that prevent C from determining the processing of its customers' data.

22 Control does not necessarily mean being in a position to determine any possible kind of
23 processing, e.g. a person may have access to a set of data and may be in a position to transfer it to
24 someone else, but the data may be protected against modification. Also, 'control' does not
25 necessarily imply that the 'controller' actually seeks access to the data or has the technical
26 capabilities that are necessary for actually accessing the data, as long as there are technical or legal
27 features that would allow that party, without unreasonable effort, to access the data if the party
28 wished to do so.

1 **Illustration:**

2 12. Company N runs a news website. Use of the website by each visitor is, with the consent
3 of N, closely monitored and recorded by data broker B (B paying a remuneration to N).
4 While company N itself never takes an interest in collecting the visitors' data, and may
5 not even have made any technical arrangements that would allow such collection, it
6 would not require unreasonable effort on N's part to do so. N therefore has control of
7 the visitors' data because it could access the data at any time if it so wished and because
8 N determines the means and purposes of their processing by allowing B to harvest the
9 data.

10 Frequently, controllers enter into contractual arrangements with other persons about the
11 processing of data to be carried out by those other persons, while keeping full control because
12 processing is carried out on their behalf and according to their directions. Such other person is a
13 processor, which means that, in some contexts—such as when it comes to the question who has to
14 comply with duties under Principle 32 or whose position counts for rightfulness under Principle
15 28—it is only the controller on whose behalf the processor is acting who counts. Being a processor
16 and processing data on behalf of a controller does not constitute control of data, so the roles of
17 ‘processor’ and of ‘controller’ are normally mutually exclusive.

18 **Illustrations:**

19 13. Business B decides to outsource payroll services with regard to B's employees and hires
20 company P to perform these services. For this purpose, relevant data (such as the
21 employees' names, wages, bank accounts or tax numbers) is processed by P on B's
22 behalf. P is not free in determining the means and, in particular, not the purposes for
23 which the employee data is processed, but rather has to follow B's directions. P is
24 therefore not a controller, but a processor.

25 14. Business B allows financial consulting firm A to access B's business data in order to
26 analyse B's business situation. A is not entirely free to determine the means and the
27 purposes of processing B's business data (e.g. A would not be allowed to disclose the
28 data to B's competitors), which could mean A is only a processor. However, A is not
29 strictly subject to B's directions either (e.g. B would not be allowed to direct A that A
30 ignores certain data in order to paint a more optimistic picture of B's business situation

1 than is the reality). Therefore it is more convincing to qualify A as controller, albeit as
2 a controller that is subject to quite rigid restrictions when it comes to the purposes of
3 the processing.

4 Employees or similar persons integrated in the controller’s organisational framework and
5 through whom the controller exercises control would not even be considered ‘processors’. When
6 the controller is a legal entity it can act only through its employees and other agents, anyway.
7 Accordingly, when an employee is merely executing decisions made by the employer, any activity
8 of the employee with regard to data should be attributed exclusively to the employer.

9 *d. ‘Co-generated data’ and ‘derived data’.* ‘Co-generated data’ means data to the
10 generation of which a person has contributed, such as by being the subject of the information or
11 the owner or operator of that subject, by pursuing a data-generating activity or owning or operating
12 a data-generating device, or by producing or developing a data-generating product or service. The
13 term is used in the context of a particular type of data rights dealt with under Chapter B of Part III.
14 The term is designed to indicate that, usually, a number of different persons have contributed to
15 the generation of data, sometimes in very different roles. There may be situations where only one
16 person has contributed, at least in a meaningful way, to the generation of data. In this situation the
17 term ‘co-generated’ may not be fully appropriate, but such a person would (*a fortiori*) have the
18 rights under Chapter B of Part III.

19 While the term ‘co-generated data’ refers to the parties who had a share in the generation
20 of data the term ‘derived data’ refers to the fact that data develops in a dynamic way and is often
21 generated on the basis of other data. Only an exact copy of a particular set of data would count as
22 the ‘same’ data, and even minor modifications would make a set of data a ‘different’ set of data. In
23 these Principles, ‘derived data’ means any data which the relevant controller has generated by
24 processing other data, i.e. by modifying, reducing, extrapolating other data or drawing inferences
25 from other data. Given that there are many different ways in which data can be generated on the
26 basis of other data and that it is so difficult to draw a clear line and provide a coherent and complete
27 set of classifications, these Principles adopt a broad notion of ‘derived’. In particular, they do not
28 differentiate between ‘derived’ and ‘inferred’ data (i.e. data generated from other data with the help
29 of external decision rules).

1 **Illustration:**

2 15. When opening a user account for an online game run by business G, users provide to
3 G their name, email address and credit card data, and G collects all sorts of other user
4 data, such as about the user’s gaming behavior, typing pace etc. G then re-structures the
5 data, fills gaps in the data and infers, with the help of algorithms and other knowledge
6 not contained in the collected data, new information from the observed data, e.g.
7 predictions about a party’s disposition to suffer from depression. The restructured data,
8 the completed data as well as the data inferred all count as derived data.

9 *e. ‘Data contracts’, ‘data rights’ and ‘data activities’.* These Principles are about data
10 contracts and data rights, so these two terms are important for the proper understanding of the
11 Principles. Both terms are to be understood broadly. A ‘data contract’ is a contract the subject of
12 which is data, either in the sense that data is the object of the transaction between two parties (i.e.
13 the data is to be transferred, disclosed, otherwise shared etc.) or in the sense that one party promises
14 to do something with regard to the data (i.e. the data is to be collected, processed, secured, etc.).

15 A ‘data right’ means a right against a controller of certain data that is specific to the nature
16 of data as a non-rivalrous resource and that arise from the way the data is generated (see Principles
17 18 to 23), or from the law for reasons of public interest (see Principles 24 to 27). It may, in
18 particular, be a right to access to or porting of this data, to correction of this data or desistance from
19 data use, or, very exceptionally, to an economic share in profits derived from using the data. Data
20 rights are, in a certain way, the data-specific corollary to the ownership rights we find in the tangible
21 world or with regard to intellectual property.

22 ‘Data activities’ is a term referred to in various places in these Principles, in particular in
23 Part IV with regard to affected third parties. It means any activities by a person with respect to data,
24 such as collection, acquisition, control, processing and other activities including onward supply of
25 data. The term is to be understood broadly, and as comprising activities of a factual (e.g. actually
26 disclosing data to another party) as well as of a legal nature (e.g. making a contract with another
27 party about access to data).

28 *f. ‘Supply’, ‘supplier’ and ‘recipient’.* It is in particular in data transactions based on
29 contract that ‘supply’ of data comes into play. The person who supplies data is the ‘supplier’ and
30 the other person is the ‘recipient.’ ‘Supply’ of data should be understood very broadly. In particular,

1 it is sufficient that the recipient gains access to the data, while it is not necessary that the recipient
2 also gains control.

3 **Illustrations:**

4 16. Company N runs a news website, offering access to world news to any visitor without
5 a paywall. N collects a wide range of data concerning the search requests and browsing
6 habits of its visitors and ‘sells’ and transfers the data to business B who will use the data
7 for profiling and scoring purposes. This involves a twofold supply: First, the news to
8 which visitors to the website of N are given access constitutes ‘data,’ and the granting
9 of access to that news is ‘supply’ of data. Second, the transfer of the data to B qualifies
10 as ‘supply’ of the visitor data.

11 17. Assume that company N in Illustration no. 16 does not collect the visitors’ data itself
12 but only allows B to collect the data on N’s site. Despite the fact that N does not
13 physically transmit any data to B, N still enables B to access the data, and to gain control
14 of the data, and therefore qualifies as a ‘supplier’ under these Principles.

15 g. ‘Transfer’, ‘porting’ and ‘erasure’. While ‘supply’ of data is a very broad and rather
16 generic term, it is often necessary to be more specific and to differentiate between different types
17 of supply. An important type of supply is ‘transfer’ of data, in which the supplier puts the recipient
18 in control of the data supplied (as contrasted with simple access). This normally implies that data
19 is to be physically stored on a medium within the recipient’s sphere of control. Note that ‘transfer’
20 does not imply that copies of the data are subsequently erased by the supplier.

21 **Illustration:**

22 18. Supply to data broker B in both Illustrations no. 16 and 17 would qualify as ‘transfer’
23 as B gets full control of the data. However, supply of the news items to visitors in
24 Illustration no. 16 would not qualify as ‘transfer’ because the visitors to the news site
25 only get access to the data and not control of the data (unless a download option is
26 offered).

27 ‘Porting’ data, which is frequently also referred to as ‘portability’ of data, means requesting
28 or otherwise initiating the transfer of data controlled by another party to oneself or to a particular
29 third party. ‘Porting’ and ‘transfer’ are thus closely related, with the main difference being that of

1 perspective, as ‘porting’ clearly takes the perspective of the recipient exercising a right, while
2 ‘transfer’ is more neutral and describes an activity of the supplier. ‘Porting’ tends to suggest to a
3 certain extent that the person requesting the transfer has a data right, i.e. that the data is, in one way
4 or another, that person’s data.

5 **Illustration:**

6 19. Supply of the data collected by N to B in Illustration no. 16 would be described as a
7 ‘transfer’ (and not as ‘porting’) because it is supplier N who collects the data and who
8 then initiates transfer to B. However, where B is allowed to harvest data from the site
9 in Illustration no. 17 and store the harvested data on B’s own medium that would be
10 described as ‘porting’ rather than as ‘transfer’, because the active part is rather played
11 by recipient B.

12 In particular contexts, ‘erasure’ of data (one type of ‘processing’ data) may become
13 relevant. This means taking reasonable steps to assure that the data is permanently inaccessible or
14 otherwise unreadable. What counts as ‘reasonable’ depends on the individual circumstances and
15 the purposes of erasure. It may, in an individual case, mean deleting all copies of the data that are
16 accessible to the person erasing the data, and, as far as possible, deleting all copies accessible to
17 third parties to whom that person has supplied the data. This is because, given the nature of data,
18 there may exist an indefinite number of copies worldwide. Sometimes it may be sufficient to press
19 a ‘delete’ button even though, strictly speaking, the data would then still remain to be retrievable
20 until the relevant storage space has been fully overwritten, and possibly even after that point. But
21 normally, more sophisticated technical measures would be required.

22 *h. Notice.* A term that is used throughout the Principles is ‘notice’. ‘Notice’ means having
23 knowledge of a fact, but also covers situations where, from all the facts and circumstances of which
24 a person has knowledge, the person can reasonably be expected to have known of the fact. It
25 includes what is often referred to as ‘wilful blindness’. Where a person has notice of a fact (e.g. of
26 the fact that processing data was wrongful) that often gives rise to an expectation that the person
27 takes action or desists from particular actions accordingly, and if the person fails to react as can
28 reasonably be expected, this often triggers adverse legal consequences.

1 *i. Definitions in other Principles.* Paragraph (2) reminds us that only those terms are defined
2 in Principle 3 that are used in various places throughout the Principles. There are other terms that
3 require a definition but that are used only in one Principle, or in one specific context, and that are
4 thus better defined in the relevant context itself. This concerns, in particular, the different types of
5 data transactions identified in Part II.

6 *j. References to ‘person’, ‘operation’ or ‘activity’.* Paragraph (3) clarifies that reference to
7 ‘person’ includes any natural or legal person, or group of persons. What may be more important is
8 that reference to any ‘operation’ or ‘activity’ includes operations and activities carried out by
9 human auxiliaries and, increasingly, by machines. Machines include any artificial intelligence, i.e.
10 it is irrelevant for the application of the Principles whether, e.g., a data contract was concluded by
11 way of two individuals exchanging offer and acceptance or whether offer and acceptance were
12 articulated and received by ‘autonomous’ software agents.

13 Needless to say, where a contract is concluded by machines some concepts used in these
14 Principles may require adaptation. For example, these Principles frequently refer to a party having
15 ‘notice’ of a fact. Where there is not a human but a machine that carries out relevant operations or
16 activities the concept of ‘notice’ may have to be adapted.

17 **Illustration:**

18 20. A contract for the transfer of particular data is made with the help of two different
19 autonomous software agents operated by supplier S and recipient R. S had received the
20 data from third party T under another contract, and under that contract S had promised
21 not to forward or disclose the data to any other person. According to Principle 34, T
22 may have remedies against R where R had ‘knowledge’ or could be expected to have
23 knowledge of S’s breach vis-à-vis T and further conditions are met. Where R used an
24 autonomous software agent and that agent was unable to process information as to
25 restrictions of that kind, R cannot hide behind the agent and claim to have been in good
26 faith.

27 Equally, any reference to intent or to standards of care, due diligence etc. may have to be
28 understood in a way that is suitable for machine-to-machine dealings. However, this is not in any
29 way different from machine-to-machine dealings other than in the context of data rights and

1 transactions, which is why these Principles do not spell out in detail how general concepts are to
2 be adapted.

3 REPORTERS' NOTES:

4 U.S.:

5 The definitions presented in this Principle are “internal” in the sense that they do not begin
6 with the defined terms and then attempt to identify their “true” or essential meaning. Rather, the
7 defined terms are more in the nature of abbreviations for broader concepts; in that context, it is not
8 the abbreviation (the defined term) itself that is important but, rather, it is the definition (the broader
9 concept) that is key. Nonetheless, inasmuch as readers cannot be expected to constantly refer to the
10 definitions in this or any other complex set of proposed rules, it is certainly desirable that the
11 defined terms convey a sense that is consistent with their definitions.

12 While these Principles are not themselves statutory in nature, they may serve as the basis
13 for future legislation. If so, the definitions presented here can serve as the basis of the definitional
14 provisions in such legislation.

15 Nomenclature concerning “data” and “information” is not standardized in the U.S. “In
16 everyday parlance, the terms “data” and “information” are often used synonymously.” Lothar
17 Determann, *No One Owns Data*, 70 *Hastings L.J.* 1 (2018). Legal distinctions between the terms
18 are often indistinct. For example, Black’s Law Dictionary defines “datum” (the singular of “data”) as
19 “a piece of information.” Black’s Law Dictionary (11th ed. 2019). The federal Electronic
20 Signatures in Global and National Commerce Act and the Uniform Electronic Transactions Act
21 define “information” as “data, text, images, sounds, codes, computer programs, software,
22 databases, or the like.” 15 U.S.C. § 7006(7); Uniform Electronic Transactions Act § 2(10) (1999).
23 They do not, however, define “data.” The same is true of the Model Computer Information
24 Transactions Act (MCITA), originally promulgated as the Uniform Computer Information
25 Transactions Act. See MCITA § 102(a)(35) (defining “information” as “data, text, images, sounds,
26 mask works, or computer programs, including collections and compilations of them”).

27 With respect to “copy,” see Model Computer Information Transactions Act § 102(a)(20)
28 (“‘copy’ means the medium on which information is fixed on a temporary or permanent basis and
29 from which it can be perceived, reproduced, used, or communicated, either directly or with the aid
30 of a machine or device.”)

31 With respect to “digital data,” see the definition of “electronic” in Principles of Software
32 Contracts § 1.01(h) (“Electronic” means technology having electrical, digital, magnetic, wireless,
33 optical, electromagnetic, or similar capabilities.).

34 Europe:

35 *a. ‘Data’ and ‘copy’.* The definitions of ‘data’ used in Europe vary significantly depending
36 on the context and the respective scientific field. In the context of the data economy, the computer
37 science understanding of data as (machine-readable) representation of information seems to be
38 gaining general acceptance (e.g. UNICITRAL, *Legal issues related to the digital economy – data*
39 *transactions* (2020); Herbert Zech, ‘„Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im

40 *digitalen Binnenmarkt*, 2015 *Gewerblicher Rechtsschutz und Urheberrecht*, p. 1151, 1153;
41 Thomas Streinz, ‘The Evolution of European Data Law’ available at SSRN:
42 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971). One of the most frequently cited
43 definitions in that regard is the one suggested by ISO/IEC 2382:2015, according to which data is

1 ‘a reinterpretable representation of information in a formalized manner, suitable for
2 communication, interpretation or processing’. The computer science understanding has also been
3 picked up by the European Commission. Both, the proposed Data Governance Act (see Article 2(1)
4 DGA, Commission Proposal COM(2020) 767 final) as well as Digital Markets Act (see Article
5 2(19) of the Commission Proposal COM(2020) 842 final) define data as ‘any digital representation
6 of acts, facts or information and any compilation of such acts, facts or information, including in the
7 form of sound, visual or audiovisual recording’. In contrast, the GDPR (Regulation (EU) 2016/679)
8 defines in Article 4(1) personal data as ‘any information relating to an identified or identifiable
9 natural person’. While the Principles follow the general trend of defining data as machine-readable
10 representation of information, it was opted to deviate from the ISO definition. In the light of the
11 many terms in this definition that tend to raise difficult questions of interpretation themselves (e.g.
12 ‘formalized’, ‘suitable for’) and of the trend towards a broader and more encompassing notion of
13 ‘processing’, the Principles adopt a simpler definition, inspired by the definition chosen by the ALI
14 Principles of the Law, Data Privacy.

15 The definition of ‘copy’ in these Principles as physical manifestation of data differs slightly
16 from the understanding of the term in EU law. In EU law, the term ‘copy’ is often used to refer to
17 an identical data set (see Articles 13(1)(f), 14(1)(f), 15(4) GDPR, Regulation (EU) 2016/679;
18 Articles 3(2), 6 Copyright Directive, Directive (EU) 2019/790). This understanding of the noun
19 corresponds in essence with the ISO/IEC 2382:2015 definition of the verb ‘copy’ as to ‘read data
20 from a source data medium, leaving the source data unchanged, and to write the same data on a
21 destination data medium that may differ from that of the source’. IEEE standard glossary: ‘To read
22 data from a source, leaving the source data unchanged, and to write the same data elsewhere in a
23 physical form that may differ from that of the source. For example, to copy data from a magnetic
24 disk onto a magnetic tape’. Principle 2(1)(b) does not deviate in substance from these definitions,
25 but rather stresses the fact that, where identical data sets are stored in different places, this means
26 that there are two or more physical manifestations on a medium.

27 *b. ‘Processing data’ and ‘access to data’.* The definition of ‘processing’ opted for in the
28 Principles is not entirely identical with the definition under EU law, notably the definition in the
29 GDPR. Article 3(2) GDPR defines ‘processing’ as any ‘operation or set of operations which is
30 performed on personal data or on sets of personal data, whether or not by automated means, such
31 as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,
32 consultation, use, disclosure by transmission, dissemination or otherwise making available,
33 alignment or combination, restriction, erasure or destruction’. Activities, such as mere viewing, or
34 disclosure as such, without any ‘physical’ operation, such as the generation of transitional copies,
35 can undoubtedly infringe a person’s privacy and thus fall under the GDPR’s definition of
36 processing. However, these activities are performed only on an intellectual level and include no
37 actual operation that is performed on the data. Hence, in the context of the data economy they
38 should not be covered by the term ‘processing’.

39 The Data Governance Act proposal is the first EU instrument to introduce a definition for
40 ‘access’. According to Article 3(8) ‘access means processing by a data user of data that has been
41 provided by a data holder, in accordance with specific technical, legal, or organisational
42 requirements, without necessarily implying the transmission or downloading of such data’. In
43 essence, this definition coincides with the Principles’ understanding of the term.

44 The term ‘access’ is also used in several sector specific regimes, e.g. Articles 61 to 66 Type
45 Approval Regulation (Regulation (EU) 2018/858); Article 36 and 66 f Payment Sector Directive
46 II (PSD II) (Directive (EU) 2015/2366); several times in the Electricity Directive (Directive (EU)
47 2019/944) and in Article 17 INSPIRE Directive (Directive 2007/2/EC), which grant parties access

1 to certain sets of data. These rights are frequently referred to as ‘data access rights’ (e.g.
 2 COM(2020) 66 final, p. 12). However, a clear terminology that distinguishes between data
 3 portability – a term used in Art 20 GDPR (see Reporters’ Notes to Principle 24.) – and data access
 4 has not been established. Therefore, the label ‘data access right’ does not necessarily imply that it
 5 gives a party less extensive rights than a portability right.

6 *c. ‘Control of data’, ‘controller’ and ‘processor’.* In Article 4(7) GDPR, ‘controller’ is
 7 defined as natural or legal person, public authority, agency or other body which, alone or jointly
 8 with others, determines the purposes and means of the processing of personal data. To an increasing
 9 extent, the term is used also with regard to non-personal data (see e.g Global partnership on AI, A
 10 Framework Paper for GPAI’s work on Data Governance, 2020). The DGA uses the term ‘data
 11 holder’, which is defined as ‘legal person or data subject who, in accordance with applicable Union
 12 or national law, has the right to grant access to or to share certain personal or non-personal data
 13 under its control’ in Article 3(5). The Principles have opted to follow this trend and thus use the
 14 same term for both personal and non-personal data and the simple noun ‘control’ to describe the
 15 position of a controller. In contrast to the DGA, a person may qualify as controller within the
 16 meaning of these Principles irrespective of whether the person has a right to determine the purposes
 17 and means of its processing. This difference can be explained by the fact the DGA’s subject matter
 18 is limited to facilitating data sharing. The DGA’s terminology would not be suitable for the
 19 purposes of these Principles, as they have a much broader scope and also address the wrongfulness
 20 of data activities.

21 Given that the concept of ‘processor’, which was originally developed by European law and
 22 has recently become widely used also in the U.S. and other parts of the world, these Principles
 23 have decided to adopt the term too. The main difference between a ‘controller’ and a ‘processor’
 24 is that the latter follows the directions given by the first, i.e. the ‘controller’ engages in processing,
 25 either by processing the data itself or by having ‘processors’ process them on its behalf. While the
 26 controller determines the purposes and means of the processing, i.e. the why and how of the
 27 processing, practical aspects of implementation (‘non-essential means’) can be left to the processor.
 28 Where the controller’s instructions leave a margin of discretion, the processor may choose technical
 29 and organizational means that best serve the controller’s interests. However, if the processor does
 30 not follow the instructions of the controller and determines own purposes and means of the
 31 processing, the processor becomes a controller (EDPD, Guidelines on the Concepts of Controller
 32 and Processor in the GDPR, 2020).

33 *d. ‘Co-generated data’ and ‘derived data’.* The term ‘co-generated data’ was coined by
 34 these Principles and has already been adopted by the European Commission in its European Data
 35 Strategy (COM(2020) 66 final, p. 10), the German Data Ethics Commission (Opinion of the
 36 German Data Ethics Commission, 2019, p. 133 ff.) and the Global Partnership on AI, GPAI (see
 37 GPAI Working Group on Data Governance, A Framework Paper for GPAI’s work on Data
 38 Governance, 2020). The underlying idea that parties who have contributed to the generation of data
 39 should have some rights in the utilization of the data is also recognized in the Japanese Ministry of
 40 Economy, Trade and Industry’s Guidelines (METI Guidelines, p 45). While the term ‘data rights’
 41 is not defined or used in EU law, it is used in more recent legal literature used to describe rights
 42 that do not clearly qualify as personality rights or property rights but lie somewhere in between
 43 (see Thomas Streinz, ‘The Evolution of European Data Law’ in Paul Craig and Gráinne de Búrca
 44 (eds), The Evolution of EU Law, 3rd edn 2021; Yuming Lian, Data Rights Law 1.0: The
 45 Theoretical Basis, 2019, p. 98 ff). This understanding corresponds with the definition chosen by
 46 these Principles.

1 Different terms have been developed to describe data resulting from different forms of
2 processing. For example, the terms ‘derived’ data and ‘inferred’ data are often used as synonyms
3 for data that was created by drawing conclusion from provided datasets (see OECD, Enhancing
4 Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies,
5 2019, p. 31; METI, Contract Guidelines on Utilization of AI and Data – Data Section, 2018, p.
6 19; EDPB, Guidelines 8/2020 on the targeting of social media users, Version 1.0, 2 September
7 2020, p. 22; see also Article 29 Data Protection Working Party, Guidelines on the right to data
8 portability, WP 242 rev.01, 5 April 2017, p. 10). ‘Aggregated data’ usually refers to the
9 combination of initially separated data sets (Bertin Martens et al., Business -to-Business data
10 sharing: An economic and legal analysis – JRC Digital Economy Working Paper 2020-05, 2020,
11 p. 5, 12). Due to lack of a clear terminology in that regard and the difficulties of drawing a distinct
12 line between derived, aggregated and structured data, the Principles have – as with the notion of
13 processing – opted for a more generic definition to cover any data resulting from any kind of
14 processing or other data activities.

15 *e. ‘Data contracts’, ‘data rights’ and ‘data activities’.* The definitions of the terms ‘data
16 contract’, and ‘data activities’ are specific to these Principles. EU legislation does not define them,
17 and no definite meanings have been attached to the terms in legal literature. However, they seemed
18 to be useful for the purpose of, in particular, Parts II and IV of the Principles.

19 *f. ‘Supply’, ‘supplier’ and ‘recipient’.* Regarding the terms ‘supply’ and ‘supplier’ reference
20 can, in particular, be made to Article 2(10) in the Proposal of the Digital Content and Services
21 Directive (COM(2015) 634 final), which defines ‘supply’ as providing access to digital content or
22 making digital content available. However, it needs to be noted that the definition was dropped in
23 the final text of the Digital Content and Services Directive (DCSD, Directive (EU) 2019/770).
24 Other documents use the term ‘data provider’ to refer to the party who provides data under a data
25 provision type contract (METI, ‘Contract Guidelines on Utilization of AI and Data – Data Section’,
26 2018, p. 19).

27 Article 4(9) GDPR, defines ‘recipient’ as a natural or legal person, public authority, agency
28 or another body, to which the personal data are disclosed, whether a third party or not. These
29 Principles use the term in a somewhat narrower sense, close to the meaning adopted by the METI
30 Guidelines, which understand data recipient to be ‘the party who receives data under a data
31 provision type contract’ (METI, ‘Contract Guidelines on Utilization of AI and Data – Data
32 Section’, 2018, p. 19).

33 *g. ‘Transfer’, ‘porting’ and ‘erasure’.* The term ‘transfer’ of data is used in Chapter V
34 GDPR and was also used in the EU-U.S. Privacy Shield (Commission Implementing Decision (EU)
35 2016/1250), which was recently discarded as void by the CJEU in its latest judgement on the matter
36 (Case C-311/18 ECLI:EU:C:2020:559 – *Schrems II*).

37 As to ‘porting’, there is no official European definition even though the term is used in the
38 heading of Article 6 Free Flow of Data Regulation (Regulation (EU) 2018/1807). In Article 20
39 GDPR, the right to ‘data portability’ is implicitly defined as the right of a data subject to receive
40 personal data which the data subject has provided to a controller, in a structured, commonly used
41 and machine-readable format, and to transmit those data to another controller without hindrance
42 from the controller to which the personal data have been provided. A similar description is provided
43 by Article 16(4) DCSD. Porting can mean transfer both to the person entitled to porting and to a
44 third party.

45 ‘Erasure’ of data is mentioned, but not defined by Article 17 GDPR. Thus, it is still under
46 discussion, whether data is erased under the GDPR, only when it is absolutely impossible to
47 retrieve the data or already when retrieving data would require unreasonable effort (see Sven

1 Hunzinger, *Das Löschen im Datenschutzrecht*, 2018, p. 55 ff). The Principles follow the latter
2 approach by setting out that ‘erasure of data means taking steps to assure, as far as is reasonably
3 possible, that the data is permanently inaccessible or otherwise unreadable’.
4 *h. ‘Notice’*. The definition of ‘notice’ is inspired by the requirement that a person ‘knew or
5 ought, under the circumstance, to have known’ a certain fact, which is a central requirement in
6 various civil law doctrines (see, for example, Article II. – 7:207 DCFR; Article 4:109 PECL on
7 excessive benefit or unfair advantage; Article VIII. – 3:101 f. DCFR on good faith acquisition of
8 ownership; Article VIII. – 3:101 f. DCFR on reversal of enrichment). At European Level, one of
9 the most conspicuous examples is probably Article 4(4) and (5) of the Trade Secrets Directive
10 (Directive (EU) 2016/943).

11 **Principle 4: Remedies**

12 **(1) Remedies with respect to data contracts and data rights, including with respect to any**
13 **protection of third parties in the context of data activities, should generally be**
14 **determined by the applicable law.**

15 **(2) Where these Principles or applicable law would mandate the return or surrender of data**
16 **by a party (the defendant) to another person (the claimant), the defendant should be**
17 **able to satisfy the obligation to return or surrender the data by, instead, erasing all of**
18 **the defendant’s copies of the data. If the claimant does not have a copy of the data, the**
19 **defendant must put the claimant in control of the data before erasing it.**

20 **Comment:** *a. Remedies.* These Principles do not generally address remedial matters,
21 leaving that to applicable law. Often, applicable law assesses money damages or monetary
22 restitution as the remedy. However, there are also a number of cases where the applicable law may
23 require specific performance, and some jurisdictions, in particular in continental Europe, may have
24 a general tendency towards preferring specific performance over money damages.

25 *b. Return as part of a remedy.* Sometimes, applicable rules or principles would require the
26 return of an item, including data, that had been delivered to a party – for example, when data has
27 been supplied by mistake, or when a contract was avoided or cancelled after data had already been
28 supplied. Return is an elusive concept for data, of which there can be many copies. Hence,
29 paragraph (2) reflects the unique character of data and adjusts the duty to return accordingly. It
30 provides that data may be ‘returned’ by erasing all copies of the data that the recipient may still
31 have under control. Where the supplier does not have a copy, e.g., because the parties had agreed

1 that the recipient would have exclusive control and the supplier had undertaken to erase all of its
2 copies, the recipient must put the supplier in control of a copy again before erasing its copies.

3 **Illustration:**

4 21. Employees of a department of company S transmit industrial data to company R in the
5 erroneous belief that a contract between S and R about the supply of the data has been
6 concluded. (Actually, negotiations had failed at the very last moment.) If applicable law
7 would otherwise require R to return the mistakenly-supplied data, R may instead erase
8 all copies of the data of which it has control. If the employees of S had erased all S's
9 copies of the data—perhaps because that was a term of the (failed) contract—R must
10 put S in control of the data before erasing it.

11 There will be situations where application of general remedial principles would lead to the
12 conclusion that data that has already been processed must be returned by the recipient. This may
13 not be reasonable and fair under all circumstances, such as, for example, when the data has been
14 processed so as to integrate it with other data in a manner that makes separation unfeasible.
15 Generally speaking, when return by erasure is unreasonable in light of the circumstances mandating
16 the return and the legitimate interests of the claimant as well as any protected third party, a court
17 should instead make a reasonable allowance in money to be paid to the supplier. Broadly speaking,
18 this is analogous to a situation in which there would be an obligation to return building materials
19 but, because the building materials have been incorporated into a structure, it would be impractical
20 to order return of the building materials so a monetary remedy is given instead.

21 **Illustration:**

22 22. If in Illustration no. 21 company R has already processed the data erroneously supplied
23 by S by way of integrating it with data from other sources and reformatting and
24 restructuring so that the data is now in the form of a searchable database from which
25 the data supplied by S cannot be separated without significant burden and expense, it
26 may be unreasonable and unfair to require R to bear that burden and expense or to erase
27 the database. However, in such a case it would equally be unfair if R were allowed to
28 keep and market the database without having to pay a reasonable amount for it, so R
29 should be required to pay S a reasonable amount of money in lieu of returning the data.

1 For an application of this concept in the context of wrongful processing see Principle 36(2).

2 **REPORTERS' NOTES:**

3 **U.S.:**

4 Under U.S. contract law, remedies for breach of contract “serve to protect one or more of
5 the following interests of a promisee:

6 (a) his “expectation interest,” which is his interest in having the benefit of his bargain by
7 being put in as good a position as he would have been in had the contract been performed,

8 (b) his “reliance interest,” which is his interest in being reimbursed for loss caused by
9 reliance on the contract by being put in as good a position as he would have been in had the contract
10 not been made, or

11 (c) his “restitution interest,” which is his interest in having restored to him any benefit that
12 he has conferred on the other party.”

13 Restatement (Second) Contracts § 344.

14 Also, “the judicial remedies available for the protection of the interests stated in § 344
15 include a judgment or order

16 (a) awarding a sum of money due under the contract or as damages,

17 (b) requiring specific performance of a contract or enjoining its non-performance,

18 (c) requiring restoration of a specific thing to prevent unjust enrichment,

19 (d) awarding a sum of money to prevent unjust enrichment,

20 (e) declaring the rights of the parties, and

21 (f) enforcing an arbitration award.”

22 Id. § 345.

23 The Uniform Commercial Code gives primacy to protection of the expectation interest. See UCC
24 § 1-305(a) (“The remedies provided by [the Uniform Commercial Code] must be liberally
25 administered to the end that the aggrieved party may be put in as good a position as if the other
26 party had fully performed but neither consequential or special damages nor penal damages may be
27 had except as specifically provided in [the Uniform Commercial Code] or by other rule of law”).

28 As for circumstances in which return of data may be an appropriate remedy, see generally
29 Restatement of the Law (Third), Restitution § 54.

30 **Europe:**

31 *a. Remedies.* With respect to data contracts, the Digital Content and Services Directive
32 (DCSD, Directive (EU) 2019/770) provides for harmonized remedies for the failure to supply
33 digital content or services, and the lack of conformity of digital content or services, in B2C
34 contracts. If the trader has failed to supply, the consumer shall call upon the trader to supply the
35 digital content or digital service. If the trader then fails to supply the digital content or digital
36 service without undue delay, or within an additional period of time, the consumer shall be entitled
37 to terminate the contract (Article 13(1) DCSD). In the case of a lack of conformity of the digital
38 content or services with the contract, the consumer shall be entitled to have the digital content or
39 digital service brought into conformity, to receive a proportionate reduction in the price, or to
40 terminate the contract (Article 14(1) DCSD). The consumer is primarily entitled to have the digital
41 content or digital service brought into conformity, and only at a secondary stage to receive a
42 proportionate reduction in the price, or to terminate the contract.

1 With the DCSD and the Consumer Rights Directive (CRD, Directive 2011/83/EU as
2 recently adapted by Directive (EU) 2019/2161) rules have been introduced also for the unwinding
3 of a contract for the supply of digital content or services after the consumer's termination, in
4 particular in cases where there is a lack of conformity with the contract. There is also a host of
5 consumer-specific remedies in other sectors, such as for the sale of goods or for package holidays.

6 Outside the realm of B2C relationships, remedies for breach of contract are mostly dealt
7 with under non-harmonized national law, which varies to a great extent. However, generally
8 speaking, the continental European legal systems favor specific performance as primary remedy,
9 and only if this fails or is inappropriate for some reason, other remedies, such as price reduction,
10 rescission or termination, or damages, would be provided. The common law jurisdictions, on the
11 other hand, take a more favorable position towards damages as the remedy that is the most
12 appropriate in many scenarios. The various general Principles that have been formulated by
13 academics at European level, such as Chapter 9 of the Principles of European Contract Law (PECL)
14 or Book III, Chapter 3 of the DCFR, tend to strike a balance between the common law position and
15 the continental position.

16 Remedies for the breach of third-party rights are not harmonized to same extent as the
17 contractual remedies. However, where a European legal system provides for non-contractual rights
18 and obligations, the same act sometimes provides remedies for the breach of these rights and
19 obligations. One example is the Enforcement Directive (Directive 2004/48/EC), which enables the
20 holder of an intellectual property right to request corrective measures (Article 11), such as the recall
21 or destruction of the goods that infringe the intellectual property right, as well as to claim damages
22 and legal costs (Articles 14 f.). Another example is the GDPR (Regulation (EU) 2016/679) which
23 entitles the data subject to an effective judicial remedy against a controller or processor (Article 79
24 GDPR).

25 Most EU instruments, however, leave the remedies for the breach of a non-contractual
26 obligation to the Member States. This is the case in the Database Directive (Directive 96/9/EC)
27 which sets out that the 'Member States shall provide appropriate remedies in respect of
28 infringements of the rights provided for in this Directive'.

29 *b. Return as part of a remedy.* Principle 4(2) is inspired by the DCSD, the CRD and the
30 Trade Secrets Directive (Directive (EU) 2016/943).

31 According to the DCSD, the consumer shall, upon termination and at the request of the
32 trader, return a tangible medium where digital content was supplied on such a medium. In any case,
33 the consumer shall refrain from using the digital content or digital service and from making it
34 available to third parties (Article 17(1) DCSD). The trader may prevent any further use of the
35 digital content or digital service by the consumer, in particular by making the digital content or
36 digital service inaccessible to the consumer or disabling the user account of the consumer (Article
37 16(5) DCSD; Article 13(8) CRD). Article 16 DCSD and Article 13(5) and (6) CRD obligate the
38 trader to make available to the consumer any content other than personal data, which was provided
39 or created by the consumer when using the digital content or digital service supplied by the trader
40 and to refrain from using the content.

41 Under Article 12(1) Trade Secrets Directive the infringer must stop the use of the trade
42 secret and destroy all or part of any document, object, material, substance or electronic file
43 containing or embodying the trade secret or, where appropriate, deliver up to the applicant all or
44 part of those documents, objects, materials, substances or electronic files.

45 The concept of the allowance of money/damages underlie the same ideas as Article 16(3)
46 DCSD, Article 13(5) CRD, Article 13 Trade Secrets Directive or Article 11 Enforcement Directive
47 (Directive 2004/48/EC).

1 The DCSD and CRD exclude, in the cases of termination or withdrawal by the consumer,
2 obligations by the trader to return consumer-generated content where such content (a) has no utility
3 outside the context of the digital content or digital service supplied by the trader; (b) only relates
4 to the consumer's activity when using the digital content or digital service supplied by the trader;
5 (c) has been aggregated with other data by the trader and cannot be disaggregated or only with
6 disproportionate efforts; or (d) has been generated jointly by the consumer and others, and other
7 consumers are able to continue to make use of the content (Article 16(3) DCSD; Article 13(5)
8 CRD).

9 However, the DCSD and CRD only exclude an obligation to erase data but do not provide
10 for an allowance in money. Such a rule can be found in Article 13 Trade Secrets Directive,
11 according to which national legislators shall provide that, at the request of the person liable to be
12 subject to measures (including erasure), the competent judicial authority may order pecuniary
13 compensation to be paid to the injured party instead of applying those measures if all the following
14 conditions are met: (a) the person concerned at the time of use or disclosure neither knew nor ought,
15 under the circumstances, to have known that the trade secret was obtained from another person
16 who was using or disclosing the trade secret unlawfully; (b) execution of the measures in question
17 would cause that person disproportionate harm; and (c) pecuniary compensation to the injured party
18 appears reasonably satisfactory. Where pecuniary compensation is ordered, it shall not exceed the
19 amount of royalties or fees which would have been due, had that person requested authorisation to
20 use the trade secret in question, for the period of time for which use of the trade secret could have
21 been prohibited.

22 According to Article 11 Enforcement Directive, a good that infringes an intellectual
23 property right shall be recalled from the channel of commerce or destroyed. However, judicial
24 authorities may order pecuniary compensation to be paid to the injured party instead of applying
25 the measures provided for in Article 11 if the liable party acted unintentionally and without
26 negligence, if execution of the measures in question would cause him/her disproportionate harm
27 and if pecuniary compensation to the injured party appears reasonably satisfactory.

28 Finally, the allowance in money is inspired by considerations that can be found in the law
29 on joint ownership in various continental legal systems (for a comparative overview see Brigitta
30 Lurger and Wolfgang Faber, *Principles for European Law - Study on a European Civil Code -*
31 *Acquisition and Loss of Ownership in Goods*, 2013, p. 1150 ff., 1180 ff.). For instance, in cases of
32 'production', i.e. when one person, by contributing labour, produces new goods out of material
33 owned by another person, the party contributing labour normally becomes the owner of the new
34 goods and the owner of the material is entitled to compensation equal to the value of the material
35 at the moment of production. Exceptionally, when the labour is of minor importance as a
36 contribution, or the producer is in bad faith, and unless the value of the labour is much higher than
37 the value of the material, ownership remains with the owner of the material and the person
38 contributing labour is entitled to the reversal of any enrichment (cf. Article VIII. – 5:201 DCFR).
39 Similar considerations also underlie the laws on unjust enrichment when it comes to the reversal
40 of enrichment. When the enriched person is no longer able to return the object of the enrichment
41 in kind, or where that would cause the enriched person unreasonable effort or expense, the enriched
42 person reverses the enrichment by paying its monetary value to the disadvantaged person (see
43 Article VII. – 5:101(2), (3) DCFR).

1 **Part II: Data Contracts**

2 **Chapter A: Rules and Principles Governing Data Contracts**

3 **Principle 5: Application of these Principles to data contracts**

4 **Data contracts under Part II should be governed, in the following order of priority, by:**

- 5 **(a) rules of law that cannot be derogated from by agreement;**
6 **(b) the agreement of the parties;**
7 **(c) any rules of the law other than those referred to in paragraph (a) that have been**
8 **developed for application to data transactions of the relevant kind;**
9 **(d) the terms included in the contracts by operation of Principles 7 to 15;**
10 **(e) application by analogy of default rules and principles of law that are not directly**
11 **applicable to data transactions of the relevant kind but that would govern analogous**
12 **transactions; and**
13 **(f) general principles of law.**

14 **Comment:** This Principle provides a general hierarchy for determining the rules governing
15 data contracts.

16 At the top of that hierarchy are mandatory rules of applicable law that cannot be varied by
17 agreement. Such mandatory rules differ from jurisdiction to jurisdiction. Examples of such rules
18 include doctrines of unconscionability or unfairness control, obligations of good faith and fair
19 dealing that cannot be disclaimed, prohibitions on excessively large liquidated damages, and also
20 certain mandatory requirements to be included in contracts between controllers and processors
21 under the law of some jurisdictions.

22 Next in priority is the agreement of the parties. This is because principles of party autonomy
23 present in most legal systems give parties to a contract wide leeway to determine the terms of their
24 relationship. Of course, what counts as the ‘agreement of the parties’ is partly an issue of fact and
25 partly the result of applying the rules of the applicable legal system as to what constitutes an
26 agreement and how binding agreements are formed, as well as rules that determine which

1 communications are to be treated as part of an agreement when varying communications, oral as
2 well as written or electronic, have been exchanged.

3 Many data transactions are the subject of extensive negotiations and careful contract
4 drafting, while others are entered into with significantly less individualized attention. Disputes
5 about the rights and obligations of parties do not typically arise when the subject of the dispute is
6 covered by express agreement of the parties. Rather, they arise more often with respect to issues
7 not covered in that agreement. All agreements are inevitably incomplete, with the result that, in the
8 event of dispute, law is called upon to fill the gaps. In some cases, the issue may be one that was
9 simply not addressed by the parties; in other cases, the parties may have thought the resolution was
10 implicit in their agreement. For issues of this sort that arise with some frequency, contract law often
11 deals with this phenomenon by providing for terms that are ‘automatically’ included in a contract
12 unless derogated from by agreement of the parties. Such terms are usually referred to as ‘default’
13 terms or ‘implied’ terms. Paragraphs (c)-(e) of this Principle set out, in order of priority, how law
14 fills the gaps in parties’ agreements in determining their rights and obligations.

15 First, paragraph (c) defers to contract law rules of the relevant jurisdiction insofar as they
16 have been developed for application to data transactions of the relevant kind. Some states may have
17 such data-specific rules, while others may not. Next, paragraph (d) refers to Principles 7 through
18 15, which develop recommended default rules for nine types of data transactions. Finally,
19 paragraph (e) provides for the application of default rules and principles that apply to analogous
20 transactions. As it is often difficult to identify contract law principles to govern a contract by
21 analogy, Principles 7 to 15 also supply a list of factors a court should consider when deciding
22 whether to adopt rules by analogy in the context of the particular types of data transactions
23 addressed in those Principles. In applying rules by analogy under paragraph (e), terms in those
24 rules should of course be adjusted to the context of data transactions. So, for example, references
25 to ownership in such rules must sometimes be replaced by references to control of the data,
26 references to use or the like replaced by references to access to data, and references to delivery or
27 the like should sometimes be read as referring to the provision of control or access. For matters not
28 addressed in paragraphs (c) to (e), paragraph (f) of this Principle ultimately defers to general
29 principles of law to fill remaining gaps. These general principles will, in the first place, be general
30 principles of contract law, but could equally be general principles of other bodies of law.

REPORTERS' NOTES:

U.S.:

Freedom of contract plays a large role in the U.S. law of contracts. See, e.g., Restatement (Second), Contracts, Introductory Note (“In general, parties may contract as they wish, and courts will enforce their agreements without passing on their substance. ... The principle of freedom of contract is itself rooted in the notion that it is in the public interest to recognize that individuals have broad powers to order their own affairs by making legally enforceable promises”).

For transactional rules of law that cannot be derogated from by agreement, see generally, e.g., UCC § 1-302. For data-specific rules of law that cannot be derogated from by agreement, see, e.g., California Consumer Privacy Act § 1798.192 (“Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer’s rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.”). Consumer protection law provides many additional examples of transactional rules that cannot be derogated from my agreement.

In addition to providing for specific rules that cannot be derogated from by agreement, U.S. contract law places limits on freedom of contract by limiting enforcement in the context of oppressive contracts and contracts the enforcement of which would be inconsistent with public policy. As to unconscionability, see UCC §§ 2-302 and 2A-108 and Restatement (Second), Contracts § 208 (“If a contract or term thereof is unconscionable at the time the contract is made a court may refuse to enforce the contract, or may enforce the remainder of the contract without the unconscionable term, or may so limit the application of any unconscionable term as to avoid any unconscionable result.”) See also MCITA § 111. As to public policy, see, e.g., Restatement (Second), Contracts §§ 178 et seq. For default rules specifically relating to data transactions, see, e.g., American Law Institute, Principles of the Law of Software Contracts (2010). For the rationale for default rules in such transactions see Model Computer Information Transactions Act , Prefatory Note:

Both MCITA and UCC Article 2 are based upon the principle of freedom of contract: with limited exceptions, the terms and effect of a contract can be varied by agreement. Ost provisions of both statutes are default rules, applicable only if the parties do not specify some other rule. Although one could try to fashion a contract code that regulates comprehensively rather than permitting such flexibility, it is hard to imagine such an approach being compatible with a vibrant market economy. Even if one succeeded in making the regulations stick, the effect would be to hinder rather than facilitate commerce. On the other hand, as noted, without certain default rules, contracting and thus legal rights remain unclear.

For one critique of applying rules from other areas of law to data transactions by analogy, see Lauren Henry Scholz, Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies (Fla. State Univ. Coll. of Law, Pub. Law Research Paper No. 895, 2018). For application by analogy of principles governing other types of transactions, see generally Daniel E. Murray, Under the Spreading Analogy of Article 2 of the Uniform Commercial Code, 39 Fordham L. Rev. 447 (1971), available at: <http://ir.lawnet.fordham.edu/flr/vol39/iss3/3>. See also, Stacy-Ann Elvy, Hybrid Transactions and the Internet of Things: Goods, Services, or Software? 74 Wash. & Lee L. Rev. 77, 117 (2017); Peter A. Alces & Aaron S. Book, When Y2K Causes “Economic Loss” to “Other Property,” 84 Minn. L. Rev. 1 (1999). As to general rules of contract law, see Restatement (Second) of Contracts (1981).

For discussions about optimal default rules in contracts, see, e.g., Oren Bar-Gill & Omri Ben-Shahar, Optimal Defaults in Consumer Markets, 45 J. L. S. S137 (2016).

1 **Europe:**
2 Freedom of contract is a fundamental principle of European Law, which is only restricted
3 by mandatory law, i.e. rules of law that cannot be derogated from by agreement, cf. Articles 1:103
4 of the Principles of European Contract Law (PECL), Article II.–1:102 of the Draft Common Frame
5 of Reference (DCFR), and Article 0:101 of the *Principes du droit européen du contrat*.

6 At European level, most of the rules on B2C contracts are of mandatory nature (see, for
7 example, Article 25 of the Consumer Rights Directive, Directive 2011/83/EU; Article 22 DCSD,
8 Directive (EU) 2019/770; Article 21 SGD, Directive (EU) 2019/771), but allow agreements that
9 are not detrimental to the consumer. In addition, unfairness control plays an important role with
10 regard to contractual clauses that have not been individually negotiated due to the Unfair Contract
11 Terms Directive (UCTD, Council Directive 93/13/EEC). For B2B contracts, the extent to which
12 jurisdictions extend unfairness control to B2B relationships varies. There are some jurisdictions
13 (e.g. German law) where unfairness control for B2B contracts is very similar to the situation in
14 consumer law, and other jurisdictions (e.g. UK law) that are heavily opposed to any interference
15 with B2B relationships. EU law takes a very cautious approach on mandatory rules so far, but there
16 is clearly a recent tendency towards an unfair contract terms control also for B2B contracts. The
17 most conspicuous examples so far may be the revised Late Payments Directive (see Article 7 of
18 Directive 2011/7/EU) or the Directive on Unfair Trading Practices in the Agricultural and Food
19 Supply Chain (Directive (EU) 2019/633). It is in a similar vein that the Platform to Business
20 Regulation (P2B Regulation, Regulation (EU) 2019/1150) provides for transparency obligations
21 the platforms have towards their business users. According to its Article 9, platform providers must
22 include in their terms and conditions a description of the technical and contractual access, or
23 absence thereof, of business users to any personal data or other data, or both, which business users
24 or consumers provide for the use of the platform services concerned or which are generated through
25 the provision of those services. Since the introduction of mandatory minimum rights and/or the
26 blacklisting of particular clauses in data law has already been considered by the European
27 Commission at an earlier stage (COM(2017) 9 final, p. 12), it would not come as a surprise if, in
28 the future EU Data Act, a proposal for which is announced for 2021 (COM(2020) 66 final, p. 13),
29 mandatory rules or blacklisted terms for B2B relations were included. However, there are also
30 tendencies towards self-regulation, e.g. in the Free Flow of Data Regulation (Regulation (EU)
31 2018/1807). According to its Article 6, the Commission shall encourage and facilitate the
32 development of codes of conduct that address data portability in B2B relationships. It is to be
33 expected that such codes of conduct, which are currently being developed (cf. COM(2018) 232
34 final p. 10 f., EU Code of conduct on agricultural data sharing by contractual agreement from April
35 2018) and which address also a number of issues besides portability rights, will establish standards
36 whose effect in practice (e.g. for purposes of unfair contract terms control, or for gap-filling) may
37 come close to the effect of default rules.

38 At national level, the effects of mandatory law on contractual agreements, such as
39 nullification of a contract, are expressed separately, often in the same provision of the code that
40 also addresses public policy. This applies to Section 879(1) of the Austrian Civil Code (‘A contract
41 that violates a legal prohibition or offends against common decency is void’) or Article 1162 of the
42 French Civil Code which states that a ‘contract may not derogate from public policy either by its
43 stipulations or by its purpose’. Similarly, under the terms of Section 134 of the German Civil Code,
44 a transaction is void if it violates a statutory prohibition.

45 While the DCSD only applies to B2C relationships, its provisions are expected to greatly
46 influence also the development of default rules for a range of data transactions. The definitions
47 given for ‘digital content’ (Article 2(1) DCSD ‘data which are produced and supplied in digital

1 form’) and ‘digital service’ (Article 2(2) DCSD: ‘a service that allows to create, process, store or
2 access data in digital form or a service that allows the sharing of or any other interaction with data
3 in digital form uploaded or created by the consumer or other users of that service’), it makes clear
4 that the focus of the DCSD is not identical with the focus of these Principles. Arguably, the DCSD
5 targets ‘functional data’, and not transactions where the ‘primary focus is on information’ (see
6 Principle 2(1)). Even though the focus of the Directive is on functional data and the fact that there
7 will only be exceptional cases where data contracts within the meaning of the Principles are
8 concluded in B2C relationships, it cannot be ignored that the broad notion of ‘digital content’ in
9 the DCSD (Article 2(1)) also covers data within the scope of these Principles. This means that, at
10 least in B2C relationships, there already exist advanced rules on ‘data contracts’ and which,
11 according to Principle 5(a), take priority over the Principles in Part II.

12 However, the DCSD does not cover all data contracts under Part II and the focus of the
13 Directive is also clearly on consumer protection, which is why it provides for very different
14 obligations for the trader (supplier) of the digital content and the consumer (recipient). The most
15 obvious overlap is with contracts for the transfer of data under Principle 7 and contracts for access
16 to data under Principle 8. However, unlike the Principles the DCSD does not contain different
17 rights and obligations depending on the mode of supply but treats both contracts the same. The
18 focus on the functional dimension of data also makes it hard to qualify contracts for the supply of
19 digital content as a contract for the transfer of data or for access to data. While it is the trader under
20 the DCSD that supplies the digital content to the consumer (as recipient), the trader can also be
21 qualified as the recipient when the consumer does not pay or undertakes to pay a price but provides
22 or undertakes to provide personal data to the trader (see Article 3(1) DCSD). This obligation could
23 somewhat be compared to contracts for the authorization to access under Principle 10.

24 The DCSD contains provisions on the mode of supply and implied warranties, including
25 concerning a recipient’s rights to receive updates, which also inspired the duties set out for the
26 supplier under Principle 7 and 8. However, the DCSD does not provide for detailed rules on control
27 and use of the supplied data by the consumer that are comparable with those set out by these
28 Principles, but only contains obligations of the consumer in the event of termination of the contract,
29 where the recipient shall refrain from using the digital content or digital service and from making
30 it available to third parties (Article 17 DCSD).

31 In continental Europe, gaps are primarily filled by non-mandatory rules (Austrian and
32 German: *abdingbare* or *dispositive Rechtsvorschriften*, Dutch: *aanvullende rechtsregels* or
33 *regelend recht*, French: *règles de droit supplétives*, Italian: *norme dispositive*, Spanish: *normas*
34 *dispositivas*) which are found in civil codes, specific statutes and in case law (cf. Hein Kötz,
35 European Contract law, 2nd Edition, 2017, p. 102 ff.) The Principles in Part II could be an
36 inspiration for the development of such non-mandatory rules on data contracts that apply in case
37 such contracts are incomplete.

38 The application of rules *per analogiam* is one of the central methodological tools at national
39 and European level (see Jörg Neuner, Judicial Development of Law, in Karl Riesenhuber (ed.),
40 European Legal Methodology, 2017, p. 291 ff). The analogous application of rules that have been
41 developed for analogous transactions has already played a major role with regard to software
42 contracts (i.e. what these Principles call ‘functional data’). Due to the narrow notion of ‘good’ in
43 some European jurisdictions, which does not cover non-rivalrous goods, contracts about software
44 would not have qualified as a sale, a lease or a service contract because the object of the transaction
45 does not qualify as a ‘good’. However, most European jurisdictions applied their rules per analogy
46 (see Reporters’ Notes to Principle 7). Similar problems will also arise when it comes to data
47 contracts under Part II of the Principles, but the main difference is that the Principles provide for

1 default rules specifically tailored to data contracts which take priority over the rules mentioned in
2 Principle 5(e).

3 Finally, data contracts are governed by the general rules and principles of contract law.
4 Such general rules and principles exist at national level, but several attempts have also been made
5 to formulate them at European level, such as by the Principles of European Contract Law (PECL),
6 the Draft Common Frame of Reference (DCFR), the ‘Principles of the Existing EC Contract Law’
7 (Acquis Principles), the *Principes du droit européen du contrat* or the ‘The Common Core of
8 European Private Law Project’ of the Trento Group. They can further be found on a more
9 international level in the UNIDROIT Principles of International Commercial Contracts (UPICC).

10 **Principle 6: Interpretation and application of contract law**

11 **In interpreting and applying rules and principles of contract law, the following factors,**
12 **among others, should be considered:**

13 **(a) the fact that data is a combination of (i) physical manifestations on a medium or in**
14 **a state of being transmitted, and (ii) information recorded;**

15 **(b) the nature of data as a resource of which there may be multiple copies and which**
16 **can be used in parallel by various parties for a multitude of different purposes;**

17 **(c) the fact that data is usually derived from other data, and that the original data set**
18 **and a multitude of derived data sets that resemble the original data set to a greater**
19 **or lesser extent may co-exist;**

20 **(d) the fact that, while the physical location of data storage may change quickly and**
21 **easily, data is normally utilized by way of remote access and the physical location of**
22 **data storage is typically of little importance; and**

23 **(e) the high significance of cumulative effects and effects of scale.**

24 **Comment:** *a. General observations.* The subject of data contracts is different, in many
25 ways, from the subject of many other contracts. Because of those differences between the subject
26 of data contracts and that of many other contracts, application of general principles of contract law,
27 often designed for those other contexts, should be sensitive to those differences. In some cases, this
28 will involve interpretation of general principles in a manner that is consistent with the context in
29 which they are to be applied. In other cases, these differences will guide and constrain analogies to
30 principles of law that govern different subjects.

1 Principle 6 comes into play at several of the levels within the hierarchy of rules established
2 in Principle 5. Where there are mandatory rules of law, i.e. rules of law that cannot be derogated
3 from by agreement, within the meaning of Principle 5(a) those mandatory rules may have been
4 drafted with traditional transactions about traditional resources (such as goods or rights) in mind.
5 When they need to be applied to a data contract, the specificities of data must be taken into account.
6 Even more, where default rules and principles of law that are not directly applicable to data
7 transactions of the relevant kind are applied by analogy within the meaning of Principle 5(e), those
8 rules and principles normally must be adapted to fit in the data context. The same holds true for
9 general principles of law, including contract law, within the meaning of Principle 5(f).

10 *b. Factors to be considered.* Principle 6 lists some factors that should be considered when
11 applying contract law that was not drafted with data transactions in mind. The most important
12 special feature of data is the fact that data is a combination of binary impulses that may be
13 physically manifest on a medium or be transmitted, and the information recorded in those binary
14 impulses. This means that, e.g., the act of supplying data is somewhat in between ‘delivering’ and
15 ‘doing’, and, accordingly, a contract to supply data is somewhat in between a sale contract and a
16 service contract.

17 **Illustration:**

18 23. If A sells a machine to B that transaction can be described as being about delivering
19 something, and if A promises to provide legal advice to B that is clearly a service.
20 However, where A shares data with B that is somewhat in between delivering something
21 to B (i.e. the binary impulses, by way of transmission) and doing something for B (i.e.
22 triggering a change in the state of B’s storage device), which makes it difficult, for
23 instance, to seek proper analogies.

24 Another important feature that makes data different from almost all other resources is its
25 non-rivalrous nature, i.e. the fact that there may be multiple copies of one and the same set of data,
26 which can be used in parallel by various parties for a multitude of different purposes.

27 **Illustration:**

28 24. Where A sells a machine to B, A will no longer have the machine, but where A sells
29 data to B, both A and B can have and use the data, and the multiplication of the data
30 does not in any way reduce its practical utility (without prejudice to the fact that the

1 market value of data may decrease rapidly with increasing numbers of persons having
2 the data). This may affect the way in which a court would apply rules and doctrines
3 such as on the passing of risk, because if data is lost or destroyed while being transmitted
4 from the supplier to the recipient the supplier is able to transmit another copy at no or
5 only negligible cost.

6 A similar feature of data is that data can be changed within fractions of a second, and that
7 almost all data is derived from other data, with the changed or derived set of data often existing in
8 parallel with all the previous versions, partly coinciding with previous versions, and partly not.

9 **Illustration:**

10 25. If A rents a cow to B it is clear that, when the contract period comes to an end, B must
11 return the cow, and, if the cow has meanwhile given birth to a calf, possibly the calf
12 (depending on the applicable contract and property law). If A gives access to data to B
13 for a particular access period the law will not only have to mandate that B erases any
14 copies of the data B may have retained (on which see the previous point as well as
15 Principle 4(2)), but will also have to decide which data sets that have, in one way or the
16 other, been derived from A's data set, are included in the duty to return.

17 Another characteristic feature of data is the fact that, while the physical location of data
18 storage may change within fractions of a second the data is normally utilised by way of remote
19 access and the storage location is of little relevance.

20 **Illustration:**

21 26. If A sells a machine to B, contract law may provide for rules on the place of
22 performance, e.g. the default rule might be that the place of performance is the place of
23 establishment of seller A, but that it is the establishment of C if the machine is currently
24 in the possession of C. However, if A supplies data to B, it may not necessarily make
25 sense to identify the place of performance according to the same rules, in particular as,
26 with cloud-based storage, the location of data may no longer play any meaningful role.
27 Indeed, the concept of a "place" of performance may have little meaning in this context.

1 Last but not least, it is the unusually high significance of cumulative effects and effects of
2 scale that make data different from other resources in that the value of data depends largely on
3 which other data they can be combined with, who has access to the data, and similar factors.

4 **REPORTERS' NOTES:**

5 **U.S.:**

6 As to the non-rivalrous nature of data, see, e.g., Charles I. Jones and Christopher Tonetti,
7 Nonrivalry and the Economics of Data (September 2019), NBER Working Paper No. w26260,
8 available at SSRN: <https://ssrn.com/abstract=3454361> (“The starting point for our analysis is the
9 observation that data is nonrival. That is, at a technological level, data is infinitely usable. Most
10 goods in economics are rival: if a person consumes a kilogram of rice or an hour of an accountant’s
11 time, some resource with a positive opportunity cost is used up. In contrast, existing data can be
12 used by any number of firms or people simultaneously, without being diminished. Consider a
13 collection of a million labeled images, the human genome, the U.S. Census, or the data generated
14 by 10,000 cars driving 10,000 miles. Any number of firms, people, or machine learning algorithms
15 can use this data simultaneously without reducing the amount of data available to anyone else”).

16 **Europe:**

17 With regard to the characteristics of data, several sets of principles stress the need to give
18 special attention to data, ensuring different treatment from goods or services, in particular in the
19 light of the non-rivalrous nature of the resource (see, for example, OECD, Data-Driven Innovation
20 - Big Data for Growth and Well-Being, 2015, p. 177 ff; OECD, Enhancing Access to and Sharing
21 of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 15 ff; European
22 Commission, A European Data Strategy, COM(2020) 66 final; German Data Strategy
23 (Datenstrategie der Bundesregierung), 2021, p. 15 ff; the French AI Strategy: Villani Report
24 (2018), p. 20 ff).

25 Both the Principles of European Law and the Draft Common Frame of Reference (DCFR)
26 state that their rules should also apply to contracts on data with ‘appropriate adaptations’ (see e.g.
27 Article 1:105 Principles of European Law, Sales; Article IV.A. – 1:101(2)(d) DCFR). However,
28 unlike Principle 6, they do not provide a list of factors that should be considered when applying
29 their rules and principles.

30 **Chapter B: Contracts for Supply or Sharing of Data**

31 **Principle 7: Contracts for the transfer of data**

32 **(1) A contract for the transfer of data is a transaction under which the supplier undertakes**
33 **to put the recipient in control of particular data by transferring the data to a medium**
34 **within the recipient’s control or by delivering to the recipient a medium on which the**
35 **data is stored.**

1 **(2) Subject to agreement of the parties and to rules that take priority pursuant to Principle**
2 **5, the law should provide that the following terms are included in a contract for the**
3 **transfer of data:**

4 **(a) With regard to the manner in which the supplier is to perform its undertaking**
5 **described in paragraph (1), the data is to be transmitted electronically to a medium**
6 **indicated by the recipient, or provided in a way enabling the recipient to port the**
7 **data to a medium of the recipient's choice, unless either that mode of delivery or the**
8 **medium indicated is unreasonable in the light of data security concerns in which**
9 **case the supplier should promptly notify the recipient of those concerns so that the**
10 **recipient may indicate a substitute mode of delivery or medium.**

11 **(b) With regard to the characteristics of the data supplied, including with regard to**
12 **nature, quantity, accuracy, currentness, integrity, granularity, and formats, as well**
13 **as with regard to the inclusion of metadata, domain tables and other specifications**
14 **required for data utilization, and to frequency of supply and any updates:**

15 **(i) The supplied data must conform to any material descriptions or**
16 **representations concerning the data made or adopted by the supplier, and to**
17 **any samples or models provided;**

18 **(ii) If the supplier has notice of the recipient's particular purpose for obtaining**
19 **the data and that the recipient is relying on the supplier's skill or judgment**
20 **in selecting the supplied data, the supplied data must be fit for the recipient's**
21 **particular purpose; and**

22 **(iii) If the supplier is in the business of supplying data of the sort that is the**
23 **subject of the contract or otherwise holds itself out as having expertise with**
24 **respect to data of that sort, the supplied data must be of a quality that would**
25 **reasonably be expected in a transaction of the relevant kind.**

26 **(c) With regard to the control of, and other data activities with regard to, the supplied**
27 **data:**

28 **(i) If the supplied data is protected by intellectual property law or a similar**
29 **regime, the supplier must place the recipient in the position of having a legal**
30 **right, effective against third parties, that is sufficient to result in the**

1 recipient's control of the data and the right to engage in such other data
2 activities that the controller had notice that the recipient could reasonably
3 expect to engage in. If putting the recipient in that position requires
4 additional steps to be taken by the supplier, such as execution or recordation
5 of a required document, the supplier must take those additional steps;

6 (ii) The supplier must place the recipient in a position, at the time the data is
7 supplied, of being able rightfully to exercise control over the data and
8 rightfully to engage in other data activities which the controller had notice
9 that the recipient could reasonably expect to engage in; if, after the data has
10 been supplied, the recipient's control of the data or other data activities
11 become wrongful this does not of itself give rise to a claim by the recipient
12 against the supplier;

13 (iii) The supplier must co-operate, to the extent reasonably necessary, in actions
14 that may be required to comply with legal requirements with respect to
15 control of the data or other data activities which the controller had notice
16 that the recipient could reasonably expect to engage in. In addition, the
17 supplier must provide to the recipient information about any legal
18 requirements with respect to any such data activities of which the supplier
19 has notice and of which the recipient cannot be expected to be aware;

20 (iv) The recipient may utilize the data and any derived data, including by onward
21 supply to others, for any lawful purpose and in any way that does not infringe
22 the rights of the supplier or third parties, and that does not violate any
23 obligations the supplier has vis-à-vis third parties provided the recipient had
24 notice of these obligations at the time the contract for the transfer of data
25 was concluded;

26 (v) As between the parties, new intellectual property rights or similar rights
27 created by the recipient with the use of the supplied data belong to the
28 recipient; and

29 (vi) The supplier may retain a copy of the data and may continue using the data,
30 including by supplying it to third parties.

1 **(3) In determining which rules and principles should apply by way of analogy to contracts**
2 **for the transfer of data, as provided in Principle 5, factors to be taken into account**
3 **should include, among others:**

4 **(a) whether the contract provides for the recipient to be in control of the data for an**
5 **unlimited period of time or for a limited period of time; and**

6 **(b) whether the contract is for a single supply of data, repeated supply, or continuous**
7 **supply over a period of time.**

8 **Comment:** *a. Scope.* Principle 7 is the first of a series of Principles setting out default
9 provisions for contracts concerning different types of data transactions. The type of data transaction
10 addressed in Principle 7 is called a ‘contract for the transfer of data’. A contract for the transfer of
11 data is a transaction under which the supplier undertakes to supply particular data to a recipient,
12 and, in doing so, to put the recipient in control of that data by transferring the data to a medium
13 within the recipient’s control or by delivering to the recipient a medium on which the data is stored.
14 This type of contract may involve data of any kind, whether raw or derived, and whether or not
15 protected by intellectual property law or a similar regime.

16 **Illustration:**

17 27. Supplier S operates an online shop and holds large amounts of customer data. S
18 promises to recipient R to supply specified types of data (name, email address, goods
19 bought, search requests made) regarding the shopping behavior of a specified number
20 (20,000) of customers from specified regions (U.S. and EU) that has accumulated over
21 a specified period (24 months) and to transfer the data to a medium within R’s control.
22 The purpose of this deal is to enable R to engage in targeted advertising campaigns.
23 This would be a contract for the transfer of data under this Principle.

24 A medium within the recipient’s control may be the recipient’s server. It may also be a
25 cloud space to which the supplier gives the recipient the access credentials if the intention is to
26 allow the recipient to download the data from the cloud space onto a medium within the recipient’s
27 control, or if the cloud space is intended to remain within the recipient’s control.

1 *b. Default terms as to the mode of supply.* The parties to a contract for the transfer of data
2 will typically agree how the data should be supplied to the recipient. If the contract is silent
3 regarding the mode of supply of the data, paragraph (7)(2)(a) provides relevant default terms. The
4 default terms provide that, generally speaking, the data is to be supplied electronically and to a
5 medium indicated by the recipient. Instead of transmitting the data directly to a medium controlled
6 by the recipient, the supplier may also provide the data on a medium to which the recipient has or
7 is given access (in accordance with Article 8(2)(a)(i)) and from which the recipient may port the
8 data to a medium of the recipient's choice. However, that mode of transfer is not required if either
9 that mode of delivery or the medium indicated by the recipient is unreasonable in the light of data
10 security concerns.

11 **Illustration:**

12 28. Assume that, in the transaction described in Illustration 27, recipient R has directed
13 supplier S to transfer the customer-related data to particular cloud space, but this cloud
14 space is insecure and, thus, not a reasonable mode of transfer. S is not obligated to
15 transfer the data to the insecure cloud space. (This protects S from the possibility that S
16 itself might be in breach of contractual and statutory duties if customer data is
17 transferred to insecure storage space.)

18 Where the mode of delivery or the medium indicated by the recipient is unreasonable in the
19 light of data security concerns the supplier should promptly notify the recipient of those concerns
20 so that the recipient may indicate a substitute mode of delivery or medium.

21 *c. Default terms as to the characteristics of the data.* When the default terms relate to
22 characteristics of the data that is the subject of the transaction, these terms are usually referred to
23 as 'warranties'. Characteristics of data have many facets, some of the most important being: nature
24 (including whether the data are personal data or non-personal data according to the applicable law),
25 accurateness, currentness, integrity, granularity, and formats, as well as the inclusion of meta data,
26 domain tables and other specifications (such as ontologies) required for data utilization, and
27 frequency of supply and any updates. The warranty terms set out in this Principle are analogous to
28 warranty terms included as default terms in contracts for the sale of goods.

29 First, in some cases, even though the parties have not expressly stated in the contract the
30 nature, quantity and quality of the data, descriptions or representations concerning the data have

1 been made or adopted by the supplier. When these descriptions or representations are part of the
2 basis of the bargain, this Principle incorporates them into the contract. In those cases, it is
3 appropriate for the supplier to be bound by those descriptions or representations as though they
4 were expressly stated in the agreement of the parties. The same holds true if the supplier has
5 provided the recipient with samples (such as a sample dataset) or models (such as the structure in
6 which the information will be presented).

7 **Illustrations:**

8 29. Assume that, in the negotiation of the transaction described in Illustration 27, supplier
9 S had stated that the data sets have been updated within the last six months. Therefore,
10 the contract includes a requirement that the data has, in fact, been updated within that
11 period.

12 30. If, during the negotiations, supplier S has provided recipient R with sample datasets of
13 100 typical customers, and in these datasets the names were complete and all the fields,
14 even the non-mandatory fields, filled in, the contract would include a term that all
15 datasets are as complete as the sample.

16 Second, if the supplier has notice of the recipient's particular purpose for obtaining the data
17 and that the recipient is relying on the supplier's skill or judgment in selecting the supplied data,
18 the supplied data must be fit for the recipient's particular purpose. In the data world, this is probably
19 an exceptional situation that is not the norm. Indeed, selecting and furnishing data in such
20 circumstances can easily be seen as an implicit statement by the supplier that the data is fit for that
21 purpose.

22 **Illustration:**

23 31. Assume that, in a situation of the kind described in Illustration no. 27, recipient R has
24 developed a new smart service that functions in conjunction with fitness bracelets from
25 a defined range of manufacturers. R is interested in having access to customers who
26 have bought such bracelets and might thus be interested in R's new service. R
27 approaches supplier S, disclosing to S this purpose and indicating that it is relying on S
28 in selecting appropriate data sets. S then declares that S has appropriate datasets for R,

1 and the two enter into a contract for the transfer of customer data. It is a term of the
2 contract that the datasets supplied are fit for the purpose disclosed by R.

3
4 Third, according to paragraph (2)(b)(ii) a default term that the supplied data must be of a
5 quality that would reasonably be expected in a transaction of the relevant kind becomes part of the
6 contract if ‘the supplier is in the business of supplying data of the sort that is the subject of the
7 contract or otherwise holds itself out as having expertise with respect to data of that sort’. This
8 condition to the presence of the default term is included because it is fair to require the supplier to
9 stand behind the quality of data in situations in which the marketplace has that expectation in light
10 of the characteristics of the supplier. This is not a mandatory term, but the burden is on a supplier
11 that does not want to have this responsibility for the quality of the data to negate the default term
12 in the contract. This arrangement of responsibilities is similar to responsibilities for the quality of
13 goods in many legal systems. One context is when the supplier is a business that collects large
14 amounts of data as part of its business, such as a social network or a search engine provider.
15 Another context occurs when a company that manufactures goods or provides services accumulates
16 a substantial amount of data as part of its operations and goes into the separate business of selling
17 that data.

18 **Illustrations:**

19 32. Shoe manufacturer S manufactures custom-made shoes for customers who supply foot
20 measurements via a specially-designed app. Accordingly, S has accumulated a large
21 amount of data about foot sizes that is not available elsewhere. S concludes that there
22 is a market for this sort of data among other shoe manufacturers, suppliers of orthopedic
23 equipment, etc., and markets the foot-size data to companies in those industries. There
24 is so much demand for this data that S makes significant profits every year supplying
25 it. S is ‘in the business of supplying data of the sort that is the subject of the
26 contract’. Accordingly the contracts for the transfer of data include the default term in
27 Principle 7(2)(b)(ii).

28 33. If, in a situation of the kind described in Illustration 27, supplier S has made trade in
29 customer data part of its business and regularly engages in this to generate additional
30 income, S can be expected to make sure the data is of the quality that is normal in

1 transactions of the relevant kind. For example, where in the relevant industry and under
2 the relevant circumstances the normal expectation would be that not more than about
3 15 percent of customer email addresses will fail at the point in time when the data is
4 transferred, the contract includes a term that the email addresses will conform to that
5 expectation.

6 34. If, conversely, in a situation of the kind described in Illustration 27, supplier S simply
7 runs an online shop and has just accumulated customer data for S's own purposes, but
8 then is approached by R whether S might be prepared to sell the customer data (which
9 S would initially not have planned, but is happy to do in order to generate additional
10 income), the term that the email addresses will conform to the expectations in the
11 relevant industry is not included in the contract.

12 *d. Default terms with regard to control of, and other data activities with regard to, the*
13 *supplied data.* A third group of default terms concerns control and use of the supplied data by the
14 recipient.

15 First, when the supplied data is protected under intellectual property law or a similar regime
16 (such as EU investment protection for databases), the supply of that data would have little value if
17 it did not include an appropriate legal right to use that data. The parties' intention is normally
18 focused on the granting or assignment of a legal right that allows the grantee or assignee to have
19 rightful control of that particular set of data, and that allows the recipient to engage in all data
20 activities which the controller had notice that the recipient could reasonably expect to engage in,
21 and that is effective vis-à-vis the rightholder and other third parties.

22 This Principle does not address whether and to what extent the supply of copyright-
23 protected software should be characterized as a license contract or as a sale; the Principle applies
24 under either characterization. The nature and extent of the right to be provided (*e.g.* whether it is a
25 license for limited or for unlimited time, on how many servers the data may be stored and run, how
26 many people may use the data at the same time), if not specified by the parties, should be broad
27 enough to enable the use contemplated by the contract. If the right provided is insufficient for such
28 use, the supplier's actions fall short of what this term requires and the supplier is liable for breach.
29 Because some domestic intellectual property regimes require licenses to be memorialized in a

1 writing or record or require recordation of the writing or record (or a reference to it), Paragraph
2 (2)(c)(i) also addresses that situation.

3 **Illustration:**

4 35. The customer data that supplier S promises to transfer to recipient R in a situation of
5 the kind described in Illustration 27 includes some photographic material that customers
6 have uploaded to share their experience with other customers and that is protected by
7 intellectual property law. Even if not expressly agreed, the contract includes a term
8 according to which S must make sure R gets a license that allows R to do at least what
9 R intends to do with the data when the contract is concluded, i.e. analyze the data for
10 purposes of targeted advertising.

11 Even where data is not protected by intellectual property law, the usefulness of data to the
12 recipient would be undermined if the recipient did not obtain rightful control over the data at the
13 time it is supplied, or could not engage in other data activities which the controller had notice that
14 the recipient could reasonably expect to engage in. Thus, paragraph (2)(c)(ii) states a default term
15 mandating that the recipient shall obtain such control. The supplier must therefore ensure that, for
16 example, there are no legal barriers that would prevent the recipient from rightfully gaining control.
17 Legal barriers could be barriers stemming, e.g., from data privacy/data protection law, from
18 intellectual property law, or from trade secrets law. The methods by which the supplier ensures the
19 absence of legal barriers will depend on the individual circumstances. They could, e.g., include the
20 seeking of valid consent or other forms of waiver of rights, or technical measures such as
21 anonymization of data.

22 **Illustration:**

23 36. Assume that, in a situation of the kind described in Illustration 27, the agreement
24 between supplier S and recipient R is silent as to whether S is responsible for assuring
25 that the customers, who are protected by a data privacy regime, have given all necessary
26 consents to transfer of control of the data to R. S supplies the data, but 5,000 of the
27 customers have not given their consent to the transfer of control of the data, with the
28 result that, under the applicable data privacy regime, control of the data by R would be
29 wrongful. S has violated its obligation under paragraph 2(c)(i) to enable the recipient
30 rightfully to exercise control over the data at the time it is supplied.

1 Unless the parties have agreed otherwise, subsequent facts rendering control or other data
2 activities by the recipient wrongful (and possibly triggering a duty of the supplier to inform the
3 recipient under Principle 32(2)), do not, as such, give rise to a claim by the recipient against the
4 supplier.

5 **Illustration:**

6 37. Same facts as Illustration 36 except that, at the time of transfer, the customers had all
7 given consent to the transfer of control of the data. After the data is supplied, however,
8 5,000 customers protected by a data privacy regime withdraw their consent to the
9 transfer, with the result that, under the applicable data privacy regime, any future control
10 or processing of these data by R would be wrongful. S has not violated its obligation
11 under paragraph 2(c)(i) to enable the recipient rightfully to exercise control over the
12 data at the time it is supplied.

13 Third, there may be other legal requirements with respect to control and use of the data.
14 Paragraph (2)(c)(iii) provides, as a default term, important obligations of the supplier with respect
15 to such requirements. In particular, the supplier is obliged to provide the sort of support that can
16 reasonably be expected in order to comply with legal requirements governing control and use of
17 the data. In addition, although a recipient can be expected to be aware of the sort of legal
18 requirements that apply to the control and use of data generally, paragraph 2(c)(ii) includes a
19 default term requiring the supplier to disclose any legal requirements that the recipient cannot be
20 expected to be aware of, as far as the supplier has notice of them, and provide support to the
21 recipient in complying with them.

22 **Illustration:**

23 38. In a situation of the kind described in Illustration 27, recipient R can be expected to be
24 sufficiently aware of the general fact that both customers from the U.S. (e.g. those
25 resident in California) and customers from the EU may be protected by data privacy
26 regimes because this is a fact that should be known to anyone engaging in a data
27 transaction. However, if it is not evident that some of the customer data qualifies as
28 health data and is therefore subject to a much stricter regime, and R (who is not a very
29 sophisticated recipient) cannot be expected to be aware of this stricter regime, S is under
30 an obligation to inform R of this fact if S has notice.

1 Fourth, unless the parties have agreed to the contrary, it is appropriate to treat the contract
2 as one that does not place any limits on how the recipient may utilize the data (including by passing
3 it on), so a default rule to that effect is included. Thus, among the policy choices for default rules
4 recommended by these Principles is that data supplied may be used by the recipient for any lawful
5 purpose that does not infringe the rights of the supplier or of third parties, including any obligations
6 the supplier has vis-à-vis third parties provided the recipient had notice of these obligations. With
7 regard to data that is not protected by intellectual property law, these Principles thus take a ‘sale’
8 approach (i.e. freedom of the recipient is the default position, and limitations must be agreed upon),
9 and not a ‘license’ approach (which would mean that, as a default rule, the recipient may engage
10 only in the data activities agreed upon).

11 **Illustration:**

12 39. As a default position, R would, in a situation of the kind described in Illustration 27,
13 be allowed to utilize the customer data for any purpose R deems fit as long as this
14 utilization does not infringe any rights of S or of third parties, including in particular
15 the customers under an applicable data privacy regime. So, provided the data privacy
16 law so allows, and there are no other specific restrictions on the use of the data (such as
17 a duty of S of which R had notice when the contract was concluded), R would be free
18 to change its mind and no longer (just) engage in targeted advertising, but instead (also)
19 use the data for developing a new online reputation system.

20 In practice, however, it is quite common that parties supply data under a contract labelled a
21 ‘license’ even where they have really concluded a contract for the transfer of data, and specify in
22 that ‘license’ the conditions under which the supplied data may be used. Where the data is not
23 protected by intellectual property law, or no longer protected due to exhaustion (first sale doctrine),
24 this is a contract covered by Principle 7 without regard to how the parties label it. Where the parties
25 make further agreements about the purposes for which the recipient may or may not process the
26 data, about the number of people to whom the data may be disclosed, or about the duration of use
27 by the recipient, they create, by virtue of freedom of contract, independent contractual obligations
28 of the recipient to refrain from particular operations.

1 **Illustration:**

2 40. If the parties in a situation of the kind in Illustration 27 so wish they may describe, in
3 some detail, the types of data use recipient R may or may not engage in. In particular,
4 they may agree that R must not compete with S on particular markets, or pass the data
5 on to third parties. R is bound by this contractual restriction on data utilization.

6 In this context, it is important to highlight the connection between Principles 7 through 15
7 and Principles 32 through 34 inasmuch as the latter deal with the supplier's obligation to pass on
8 certain restrictions and obligations to the recipient and to alert the recipient, (e.g., if subsequent
9 events occur that are relevant for the recipient's legal position). In particular, Principle 32(1)
10 obliges the supplier to impose particular contractual duties and restrictions on the recipient to the
11 extent that these duties and restrictions must be complied with for the benefit of a protected party
12 within the meaning of Part IV Chapter A.

13 Fifth, the question of allocation of intellectual property rights created with supplied data is
14 something parties to a transaction should normally agree on in advance, inasmuch as that allocation
15 may have important economic effects. Under this Principle there is a default term that these new
16 intellectual property rights belong to the recipient. As with all default terms, this is subject to
17 mandatory legal rules that cannot be derogated from by contract, and to agreement between the
18 parties to the transaction. For example, applicable law might provide that new intellectual property
19 rights are vested in a third party such as in an employee of the recipient.

20 **Illustration:**

21 41. Assume that in a situation of the kind described in Illustration 27 R would indeed use
22 the data for developing a new online reputation system, which in itself would be
23 protected by copyright. As a default position, S would not hold any rights in that system,
24 and all intellectual property rights would be vested in R. This is, however, just as
25 between the parties, so if the law provides that, really, the intellectual property rights
26 should be vested in independent coder C this is to be respected.

27 Sixth and finally, a contract for the transfer of data is not usually intended to deprive the
28 supplier of the continuing right to use that data. Accordingly, paragraph (2)(c)(vi) provides a
29 default rule to the effect that the supplier may retain a copy of the data and may continue using it,

1 including by supplying it to third parties, i.e., any utilization rights of the recipient are normally
2 non-exclusive.

3 **Illustration:**

4 42. In a situation of the kind described in Illustration 27, no one would expect supplier S to
5 delete all its customer data after having transferred them to recipient R. But there may
6 be scenarios where this is less self-evident, e.g. where the data relate to a type of goods
7 S wishes to stop offering on the market, while R wants to invest into selling precisely
8 this type of goods. Still, in the absence of an agreement to the contrary, S would not be
9 required to delete the data after the transfer.

10 *e. Application of other law by analogy.* Principle 5 provides that default rules and principles
11 that are not directly applicable to the transaction at hand but that would govern a type of transaction
12 akin to the transaction at hand may be applied to the transaction at hand by analogy.

13 Since a contract for the transfer of data under which the recipient may use the data for an
14 unlimited period of time will very often have many important characteristics of a sale, inasmuch
15 as unlimited use transfers the economic value of the data to the recipient, the closest analogy may
16 often be to the law of sale of goods, unless the relevant jurisdiction provides for specific rules on
17 the supply of digital content. Where, however, the terms of the contract provide that the recipient
18 may use the data only for a limited period of time (whether or not enforced by the data being self-
19 destructing and readable only for a limited period of time) the more appropriate analogy may
20 sometimes be the law of lease contracts, or similar bodies of the law. Also, different sets of legal
21 rules may apply depending on whether the contract is for a one-time exchange or for repeated or
22 continuous supply.

23 The list of criteria to take into account when deciding which rules and principles to apply
24 by analogy provided in paragraph (3) is not exhaustive. Other criteria that may be useful, depending
25 on the circumstances, include the nature of the data and of any third-party rights in the data, and
26 whether the supplier also promises, under the same contract, to customise the data sets that are to
27 be supplied, which may recommend an analogy to the law of services contracts.

1 **REPORTERS' NOTES:**

2 **U.S.**

3 The terms included in a contract for the transfer of data under paragraph (1) can be
4 analogized to the delivery terms in UCC § 2-503 *et seq.* See also, Model Computer Information
5 Transactions Act § 606. (In the 1990s, the American Law Institute and the Uniform Law
6 Commission (the co-sponsors of the U.C.C.) engaged in an effort to draft a uniform law that would
7 govern many information transactions directly, with rules tailored specifically for that context. It
8 was intended that the law would become part of the Uniform Commercial Code known as “Article
9 2B – Software Contracts and Licenses of Information.” The effort foundered however, with the
10 ALI withdrawing from the project in 1999. The Uniform Law Commission continued the project
11 separately, promulgating it in revised form as the Uniform Computer Information Transactions
12 Act, but efforts at enactment have been unsuccessful with two enactments in 2000 and none since.
13 The product has since been renamed as the Model Computer Information Transactions Act.) The
14 terms that are included in a contract for the transfer of data under paragraph (2) would typically be
15 referred to under U.S. contract law as implied terms.

16 The terms related to the characteristics of the data in paragraph (2)(a) are parallel to implied
17 warranties under UCC Article 2 in the context of the sale of goods and under Article 2A in the
18 context of the lease of goods:

19 1. Descriptions or representations concerning the data that have been made or adopted by
20 the supplier and have become part of the basis of the bargain would, if the subject of the contract
21 were goods, be considered express warranties. See UCC §§ 2-313, 2A-210. See also Model
22 Computer Information Transactions Act § 402; ALI Principles of Software Contracts § 3.02.

23 2. When the seller or lessor of goods is a “merchant,” the contract of sale or lease contains
24 an implied warranty that the goods are “merchantable.” To be merchantable, goods must satisfy
25 several criteria including, most important for this context, that the goods would pass without
26 objection in the trade and be fit for the ordinary purposes for which such goods are used. See UCC
27 §§ 2-104, 2-314 and 2A-212. See also Model Computer Information Transactions Act § 403; ALI
28 Principles of Software Contracts § 3.03

29 3. When a seller or lessor of goods has reason to know the particular purpose of the buyer
30 or lessee and that the buyer or lessee is relying on the skill or judgment of the seller or lessor to
31 select or furnish suitable goods, there is an implied warranty that the goods are fit for that purpose.
32 See UCC §§ 2-315 and 2A-213. See also Model Computer Information Transactions Act § 405(a);
33 ALI Principles of Software Contracts § 3.04

34 4. When goods are sold or leased, there is a warranty of title and against infringement
35 implied in the contract. See UCC §§ 2-312 and 2A-211. See also Model Computer Information
36 Transactions Act § 401; ALI Principles of Software Contracts § 3.01

37 In addition to the Model Computer Information Transactions Act, reference should be made
38 to the ALI’s Principles of the Law of Software Contracts, which addresses many of the same issues
39 addressed in the Model Act, albeit not always reaching the same conclusion.

40 Courts have, on occasion, applied UCC Article 2 by analogy to transactions outside its
41 formal scope such as data and software contracts. See, *e.g.*, *Arbitron, Inc. v. Tralyn Broadcasting,*
42 *Inc.*, 400 F.3d 130, 138 & n.2 ((2d Cir. 2005); *i.Lan Systems, Inc. v. Netscout Service Level Corp.*,
43 183 F.Supp.2d 328 (D. Mass. 2002). See generally Murray, *Under the Spreading Analogy of*
44 *Article 2 of the Uniform Commercial Code*, 39 Ford.L.Rev. 447 (1971).

1 **Europe:**

2 *a. Scope.* ‘Contracts for the supply of data’ do not fall under any of the established contract
3 types in continental European legal systems. However, EU law has a clear tendency to treat the
4 supply of digital content similar to sales contracts. In its decision *UsedSoft* (Case C–128/11
5 *UsedSoft* ECLI:EU:C:2012:407), the CJEU clarified that the supply of a computer program for an
6 unlimited time against remuneration is to be considered a ‘sale’ within the meaning of the Software
7 Directive (Directive 2009/24/EC) and thus exhausts the copyright holder’s distribution right for
8 that copy. Regarding remedies for lack of conformity of supplied digital content and services, the
9 DCSD (Directive (EU) 2019/770) has introduced a uniform, sales-like regime.

10 Specific provisions for the transfer of data, however, do exist with regard to personal data.
11 The European Commission has adopted so-called Standard Contractual Clauses (SCC) for the
12 transfer of personal data to controllers and processors established in third countries (Commission
13 Implementing Decision (EU) 2021/914). Where an exporting controller and an importing controller
14 or processor include the SCC in their contract, the transfer of the data outside the EU is considered
15 to be in accordance with EU data protection legislation, but a recent judgment of the CJEU (C-
16 311/18 ECLI:EU:C:2020:559 – *Schrems II*) may mean that further steps are often required. While
17 SCC are not contract law that governs the parties’ contractual relationship without any agreement
18 to that end, they provide important indications as to what the European legislator considers to be a
19 reasonable and fair contractual arrangement.

20 *b. Default terms on mode of supply.* Given that there is not much in terms of specific rules
21 on the supply of data in European legal systems the main source for Principle 7(2)(a) is Article
22 5(2) DCSD. It provides that the trader shall have complied with the obligation to supply digital
23 content or services where (a) the digital content or any means suitable for accessing or downloading
24 the digital content is made available or accessible to the consumer, or to a physical or virtual facility
25 chosen by the consumer for that purpose; or (b) the digital service is made accessible to the
26 consumer or to a physical or virtual facility chosen by the consumer for that purpose. The fact that
27 this provision does not include a reservation as to data security can easily be explained by the types
28 of scenarios which the DCSD has been designed to address, i.e. mass contracts with consumers,
29 where the trader fully controls the mode of supply anyway.

30 *c. Default terms as to the characteristics of the data.* The warranties laid down in Principle
31 7(2)(b) mirror to some extent the DCSD’s conformity requirements for digital content and services.
32 Traditionally, European legal systems differentiate between a subjective conformity test and an
33 objective conformity test. According to Article 7 DCSD, subjective requirements for conformity
34 are that the digital content or service (a) is of the description, quantity and quality, and possess the
35 functionality, compatibility, interoperability and other features, as required by the contract; (b) is
36 fit for any particular purpose for which the consumer requires it and which the consumer made
37 known to the trader at the latest at the time of the conclusion of the contract, and in respect of which
38 the trader has given acceptance; (c) is supplied with all accessories, instructions, including on
39 installation, and customer assistance as required by the contract; and (d) is updated as stipulated by
40 the contract. The objective requirements for conformity listed in Article 8 DCSD include that the
41 digital content or service (a) is fit for the purposes for which digital content or digital services of
42 the same type would normally be used, taking into account, where applicable, any existing law,
43 technical standards or sector-specific industry codes of conduct; (b) is of the quantity and possesses
44 the qualities and performance features, including in relation to functionality, compatibility,
45 accessibility, continuity and security, normal for digital content or digital services of the same type
46 and which the consumer may reasonably expect, given the nature of the digital content or digital
47 service and taking into account any public statement made by or on behalf of the trader, or other

1 persons in previous links of the chain of transactions, particularly in advertising or on labelling; (c)
2 is supplied along with any accessories and instructions which the consumer may reasonably expect
3 to receive; and (d) complies with any trial version or preview of the digital content or digital
4 service, made available by the trader before the conclusion of the contract.

5 *d. Default terms with regard to control of, and other data activities with regard to, the*
6 *supplied data.* Similar to Principle 7(2)(c)(i), the DCSD lays down an obligation to supply the
7 recipient with digital content or services that are free from any third party rights. Article 10 DCSD
8 provides that where a restriction resulting from a violation of any right of a third party, in particular
9 intellectual property rights, prevents or limits the use of the digital content or digital service in
10 accordance with the contract the consumer shall be entitled to remedies for lack of conformity
11 unless national law provides for the nullity or rescission of the contract for the supply of the digital
12 content or digital service in such cases. Similar provisions can be found in national sales laws or
13 laws of obligations, (cf. Section 933 of the Austrian Civil Code; Article 7:15-7:16 of the Dutch
14 Civil Code; Article 217(2)(4) of the Estonian Law of Obligations Act; Article 41(1) of the Finland
15 Sales Act; Section 435 of the German Civil Code; Section 41 UK Consumer Rights Act).

16 In contracts for the sale of goods (cf. Article 10(1) CSD II (Directive (EU) 2019/771);
17 Article IV.A – 5:102 DCFR; Article 42 CISG), the risk passes when the goods are supplied under
18 Principle 7(2)(c)(ii). The limitation that developments after the data has been supplied, do not of
19 itself give rise to a claim by the recipient against the supplier can also be found in Article 11(2) of
20 the DCSD, according to which the trader shall normally be liable only for any lack of conformity
21 which exists at the time of supply.

22 As to the supplier’s duties to support the recipient in complying with all legal requirements
23 with respect to control of the data, as can reasonably be expected, including by providing
24 information (Principle 7(2)(c)(iii)), most European jurisdictions would qualify this as an ancillary
25 obligation under the contract. Article 1:202 PECL provides for a general duty to co-operate which
26 each party owes to the other in order to give full effect to the contract (See also Article III. – 1:104
27 DCFR). European data protection law recognizes a duty of the recipient of personal data to support
28 the supplier in complying with all legal obligations. Article 28(3) GDPR provides that the processor
29 must, inter alia, assist the controller by appropriate technical and organizational measures, insofar
30 as this is possible, for the fulfilment of the controller's obligation to respond to requests for
31 exercising the data subject's rights and in ensuring compliance with legal obligations. Furthermore,
32 Clause I(c) of the SSC (Commission Decision 2004/915/EC) provides that a person exporting data
33 outside the EU shall provide the data importer, when so requested, with copies of relevant data
34 protection laws or references to them.

35 As to the recipient’s general legal position, Principle 7(2)(c)(iv) follows a ‘sales approach’
36 rather than a ‘license approach’. Hence, it is set out that the recipient is generally entitled to use
37 the data for any lawful purpose.

38 The attribution of intellectual property rights for newly created content to the recipient
39 (Principle 7(2)(c)(v)) is based on the idea that, normally, the recipient is the one who will make the
40 essential intellectual effort for the development of these rights. Under European law, intellectual
41 property rights will therefore normally be vested in the recipient anyway (see Articles 2 – 4
42 Information Society Service Directive, Directive 2001/29/EC; Article 2(2) Rental and Lending
43 Directive, Directive 2006/115/EC; Article 2(1) Software Directive, Directive 2009/24/EC). The
44 policy choice to attribute newly created content to the recipient is also reflected in European
45 contract law. According to Article 16(4) DCSD, the consumer can, after the termination of the
46 contract, request any content which was created by the consumer when using the digital content or
47 digital service supplied by the provider.

1 Due to its non-rivalrous nature, data can be used simultaneously by various actors without
2 exhausting the resource. Hence, Principle 7(2)(c)(vi) provides a default rule to the effect that the
3 supplier may retain a copy of the data and may continue using it, including by supplying it to third
4 parties.

5 *e. Application of other law by analogy.* Since the implementation of the DCSD the most
6 appropriate analogy in Europe will usually be with contracts for the supply of digital content or
7 digital services. In B2B cases, the relevant rules must be distinguished from any consumer-specific
8 policy decisions. However, national courts may, for B2B cases, also retain the solutions they had
9 developed before the DCSD was issued. Many European legal systems apply rules on sales *per*
10 *analogiam* also to the supply of digital content if the recipient can use the content for an unlimited
11 period. The provisions for lease contracts are often applied if the use is limited to a certain (albeit
12 possibly indefinite) period and the rules for service contracts if the digital content is customized.
13 For example, the Principles of European Law and the Draft Common Frame of Reference (DCFR)
14 apply with appropriate adaptations, to contracts for the sale or barter of information and data,
15 including software and databases, except where the buyer is only given a license to use the software
16 (see e.g. Article 1:105 Principles of European Law, Sales; Article IV.A. – 1:101(2)(d) DCFR). The
17 Principles of European Law further clarify that the sales provisions are also applied *per analogiam*
18 to the transfer of information ‘to the extent that it is a standard affair.’ However, if the transaction
19 involves a request for evaluative information, it will be qualified as a service.

20 **Principle 8: Contracts for simple access to data**

21 **(1) A contract for simple access to data is one under which the supplier undertakes to**
22 **provide to the recipient access to particular data on a medium within the supplier’s**
23 **control and which is not a contract for the transfer of data under Principle 7. This**
24 **includes contracts where the supplier, in addition to enabling the recipient to read the**
25 **data, undertakes to put the recipient in a position to process the data on the medium**
26 **within the supplier’s control, or port data.**

27 **(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the**
28 **law should provide that the following terms are included in a contract for simple access**
29 **to data:**

30 **(a) With regard to the mode of the recipient’s access to the data:**

31 **(i) The supplier must provide the recipient with the necessary access**
32 **credentials and remove any technical barriers to access whose removal could**
33 **reasonably be expected in a transaction of the relevant kind;**

- 1 (ii) The supplier must make the data accessible in a structured and machine-
2 readable format of a sort that can reasonably be expected in a transaction
3 of the relevant kind;
- 4 (iii) The supplier must enable the data to be accessed remotely by the recipient
5 unless this is unreasonable in the light of data security concerns;
- 6 (iv) The recipient may process the data to which the recipient is given access only
7 for purposes consistent with any purposes agreed in the contract;
- 8 (v) The recipient may port data to which it is given access in the contract only
9 when the porting of such data can reasonably be expected in a transaction
10 of the relevant kind and may port data derived from the recipient's
11 processing activities carried out in accordance with the contract (e.g, data
12 derived from data analytics); and
- 13 (vi) The recipient may read the data, process or port the data, as applicable, by
14 any means, including automated means, and may do so as often as the
15 recipient wishes during the access period agreed.
- 16 (b) With regard to the characteristics of the data to which access is provided, the terms
17 listed in Principle 7(2)(b) for contracts for transfer of data also apply in a contract
18 for simple access to data.
- 19 (c) With regard to the control of any data ported by the recipient in accordance with
20 the contract, and other data activities, the terms listed in Principle 7(2)(c) for
21 contracts for transfer of data also apply in a contract for simple access to data.
- 22 (3) In determining which rules and principles to apply by way of analogy, as provided in
23 Principle 5, to contracts for simple access to data, consideration should be given in
24 particular to the degree to which the recipient may only view the data, may process data
25 on the medium within the supplier's control, or may port data.

26 **Comment:** *a. Scope* This Principle covers contracts where the obligation assumed by the
27 supplier is to give the recipient access to data on a medium within the supplier's control. Parties
28 may wish to choose a contract for simple access to data where they do not want the recipient
29 obtaining full control of (all) the data that are the object of the bargain. This can be for data

1 privacy/protection, data security or other reasons, in particular in light of the fact that data that has
2 once been transferred to a recipient can hardly be recovered if used or passed on by the recipient
3 in breach of the terms agreed. Contracts for simple access to data do not fall under Principle 7, but
4 are covered in Principle 8 (and, to a certain extent, in Principle 9). The main difference between
5 contracts within Principle 7 and those within this Principle is that, under the latter, the supplier
6 does not transfer the data to a medium under the control of the recipient but, rather, gives the
7 recipient access to a medium under the supplier's control on which the data is stored.

8 **Illustration:**

9 43. Car manufacturer S conducts intensive research on the development of new car models,
10 collecting vast amounts of test data on various prototypes and their components. The
11 data would enable engine manufacturer R to learn better how its engines operate and
12 how they can be improved. S is willing to enter into a contract with R that would enable
13 R to obtain that benefit but, in light of the vast investment made by S into the research
14 and the risk that any data transferred to R will be passed on to competitors or hacked by
15 third parties, S is reluctant to transfer the test data to R. Rather, the parties agree that R
16 will have access to a defined class of test data on S's servers. The contract effectuating
17 this agreement is a contract for simple access to data under this Principle.

18 44. Same facts as Illustration 43 except that the contract requires S to upload the data to R's
19 server. The contract is a contract for the transfer of data under Principle 7.

20 Contracts for simple access to data can involve situations in which the recipient is provided
21 read-only access, as well as those in which the recipient may process the data on the medium within
22 the supplier's control or port particular data. As the key motivation for suppliers to enter into a
23 contract for simple access to data covered by Principle 8 rather than into a contract for the transfer
24 of data covered by Principle 7 is typically for the supplier to remain in full control of the data, this
25 motivation may be served best if access is provided to the recipient on a read-only basis. However,
26 a read-only basis is often not sufficiently useful for the recipient. This is why parties frequently
27 agree that the recipient is permitted not only to read the data but also to process the data on the
28 medium within the supplier's control or port particular data. Such contracts also fall under Principle
29 8.

1 **Illustration:**

2 45. In order to benefit from the test data and be able to improve its engines, R in Illustration
3 43 would need to conduct its own research using the data. Accordingly, S and R agree
4 that R may run its own data analytics on S's servers, thus engaging in data processing
5 on a medium controlled by S. Because R wants to use the results of such data analytics
6 in R's own factory, S and R agree that R may port the results of data analytics,
7 transferring those results to R's own servers. The contract is a contract for simple access
8 to data under this Principle.

9 Obviously, the greater the portion of data the recipient is allowed to port the more similar
10 in effect the transaction will be to a contract for the transfer of data under Principle 7.

11 *b. Default terms with regard to the mode of the recipient's access to the data.* The default
12 terms in Principle 8(2)(a) regarding the mode of the recipient's access to the data are necessarily
13 more complex than the terms stated in Principle 7 with respect to the mode of supply.

14 First, since the access will typically be secure, Principle 8(2)(a)(i) states that the supplier
15 must provide the recipient with the necessary access credentials and remove any technical barriers
16 whose removal could reasonably be expected in a transaction of the relevant kind.

17 **Illustration:**

18 46. Assume that, in Illustration 43, S provides R with the access credentials, but when R
19 tries to access the data it turns out that R can read the data, which is encrypted, only if
20 R is prepared to buy very special and expensive decryption software used by S but not
21 common in R's industry. S could easily decrypt the data itself. R has a right against S
22 that S remove the technical barrier posed by the encryption.

23 Second, Principle 8(2)(a)(ii) supplies a default term as to the format in which the data is to
24 be accessible. Under that term, the data must be accessible in a structured and machine-readable
25 format that can reasonably be expected in transactions of the relevant kind.

26 Third, the default term in Principle 8(2)(a)(iii) provides that the recipient may access the
27 data remotely unless this is unreasonable in the light of data security concerns. Of course, in some
28 cases the parties may agree that the recipient is allowed to view the data only locally, e.g. where
29 the data is saved on a server without internet connection.

1 **Illustration:**

2 47. Assume that in a situation such as the one in Illustration 43, when R requests remote
3 access to S's server for the first time, S denies access, claiming that its internal security
4 policies only allow such data to be accessed locally. Instead, S insists that R's
5 employees must travel to S's premises whenever R intends to access the data. According
6 to the default term in Principle 8(2)(a)(ii), S is allowed to deny access to R only if
7 remote access was, in light of the sensitivity of the data and the inherent insecurity of
8 the internet connections available to R, objectively unreasonable, and not just according
9 to S's internal policies.

10 Fourth, Principle 8(2)(a)(iv) provides that the recipient may process the data to which the
11 recipient is given access only for purposes that are consistent with the purposes agreed in the
12 contract. This default term different from the default term provided in Principle 8(2)(c) for data to
13 be ported (the latter being the same as under Principle 7(2)(c)(iv)). The reason is that the likely
14 primary motivation for parties to enter into a contract for simple access to data under this Principle
15 instead of into a contract for the transfer of data under Principle 7 is that the supplier wants to
16 remain in control, in particular due to data security or data privacy/data protection concerns, or any
17 other necessity to remain abreast of data activities with regard to the data in question.

18 **Illustration:**

19 48. Assume that in a situation such as the one in Illustration 43, the parties originally
20 envisaged in their contract that R would engage in certain processing activities to learn
21 better how its engines operate and how they can be improved. However, when analyzing
22 the data, R realizes that there is huge potential in the data for developing a new
23 recommender system for connected cars. Given that this purpose is different from the
24 purpose agreed in the contract, and might potentially harm S's interests (e.g., if S itself
25 is developing such a service), R cannot simply process the data for that purpose but has
26 to seek an extended agreement with S.

27 Fifth, Principle 8(2)(a)(v) addresses which data the recipient is allowed to port. Given that
28 porting data is likely to undermine the motivation of the parties for choosing a contract under this
29 Principle instead of a contract for the transfer of data under Principle 7, this default term is rather
30 restrictive. Under this term, the recipient may port only such data as the recipient could reasonably

1 expect to be allowed to port in a transaction of the relevant kind. Principle 8(2)8a(v) also supplies
2 a default term that, if the recipient is entitled to process the data (e.g. by analyzing it) on the
3 supplier's medium, the recipient may also port the derived data.

4 **Illustration:**

5 49. According to the contract between S and R in Illustration 43, R is allowed to run its
6 own data analytics with its own software in a workspace on S's servers in order to learn
7 more about the performance of its engines. However, after the data analytics has been
8 completed and R asks S for the credentials required for porting the results S claims that
9 porting of any data had never been part of the contract and that R would be allowed to
10 port the results of the analytics only if R is prepared to pay a significant extra sum of
11 money. Even if the contract is silent, R has a right to port the data derived from its own
12 processing activities.

13 Sixth, Principle 8(2)(a)(vi) provides a default term that, as is typical in contracts for simple
14 access to data, the recipient may read, process, or port the data by any means, including automated
15 means, and as often as the recipient wishes during the agreed access period.

16 **Illustration:**

17 50. Assume that in a situation such as the one in Illustration 43 R accesses the data with
18 the help of advanced artificial intelligence, which, within only very few hours, analyses
19 all the data made accessible to R. S had not anticipated this and claims that this sort of
20 access was improper and that, if R had disclosed its intentions during the negotiations,
21 the price for the access would have been much higher. As the parties have left this point
22 open the default position is that R was entitled to access the data with the help of AI.

23 *c. Default terms with regard to the characteristics of the data supplied.* Principle 8(2)(b)
24 indicates that, with respect to the characteristics of the data supplied, the supplier has the same
25 responsibilities as it would have in a contract for the transfer of data. See Principle 7(2)(b). This
26 reflects the view that there are no policy reasons for differentiating between a contract for the
27 transfer of data and a contract for simple access to data with respect to these issues. As with the
28 default terms stated in Principle 8(2)(a), the parties are free to vary from these terms by agreement.

1 (ii) **Access to the data is provided in real time as the data is collected or generated**
2 **by the data source.**

3 **(b) With regard to the characteristics of the data, there is no requirement that the**
4 **recipient will receive data of a particular quality or quantity.**

5 **(3) In determining which rules and principles to apply by way of analogy, as provided in**
6 **Principle 5, to contracts for exploitation of a data source, consideration should be given**
7 **in particular to:**

8 **(a) the degree and duration of control which the recipient is to receive over the data**
9 **source; and**

10 **(b) whether, and the degree to which, the recipient may port data.**

11 **Comment:** *a. Scope.* Under a contract for exploitation of a data source within the meaning
12 of Principle 9 the supplier undertakes to provide to the recipient access to data by giving the
13 recipient access to a device or facility by which data is collected or otherwise generated. A contract
14 for exploitation of a data source is thus a special type of a contract for access to data, focussing on
15 access to, and usually processing and/or porting of, data collected or generated by the data source.
16 Thus, the focus of the transaction is the data source rather than the characteristics of the data. If a
17 contract is about access to particular (existing) data, it is not a contract for exploitation of a data
18 source addressed by this Principle, but a contract for the simple access to data under Principle 8.
19 Contracts for the exploitation of a data source are common in the data economy.

20 **Illustrations:**

21 51. Car manufacturer C makes a contract with business B under which B is granted access
22 to the data generated by the connected cars' windshield wipers and headlights, which
23 in turn enables B to provide exact weather reports even for areas where no other weather
24 sensor data is available. Neither C nor B know how much the car owners will drive their
25 cars and where and when they will drive them, and C does not make any promise to B
26 in that regard. Since B is granted access to the facility by which data is produced and
27 the contract is not one for access to data under Principle 8, the contract is thus one for
28 exploitation of a data source.

1 52. Company N runs a news website. Use of the website by every visitor is, under
2 contractual agreements with N, closely monitored and recorded by data broker B. B will
3 use the data for profiling and scoring purposes. The agreement between N and B is a
4 contract for exploitation of a data source because neither N nor B knows exactly how
5 many visitors will use the website and there is no requirement that there be any
6 particular number of visitors.

7 The technical arrangements for providing the recipient with access to the device or facility
8 as described in paragraph (1) may vary. In particular, it is not necessary that the supplier gives the
9 recipient access to the ‘original’ data source. Very often, the parties will agree that the data may be
10 transferred from the original data source to a kind of ‘duplicate’ of that source, to which the
11 recipient is then provided access.

12 **Illustration:**

13 53. In a case such as the one described in Illustration 51, car manufacturer C does not wish
14 to give B direct access to its car fleet. Rather, the parties agree to an arrangement
15 according to which C initiates automatic and continuous transfer of any data generated
16 by the windshield wipers and headlights to a server space to which B is then granted
17 access. While this server space is not really the ‘data source,’ the parties have made it a
18 ‘duplicate’ of the original data source. Accordingly, the contract is one for exploitation
19 of a data source.

20 *b. Default terms.* The default terms included in a contract for exploitation of a data source
21 are, as a starting point, the same as under Principle 8. However, there are three additional terms
22 complementing or concretising the terms listed in Principle 8(2). In particular, where the default
23 terms in Principle 8(2) refer to what can ‘reasonably be expected in a transaction of the relevant
24 kind’, the fact that the nature of the transaction is one for exploitation of a data source rather than
25 one for access to particular data is relevant in determining those reasonable expectations. More
26 precisely, in a contract for exploitation of a data source under this Principle, there are two specific
27 default terms, i.e. that the recipient is (i) permitted to access and port all data generated by the data
28 source, and (ii) given real-time access to the data as the data is generated, or as close to real time
29 access as is reasonably possible.

Illustration:

54. Assume that, in Illustration 53, a certain part of the data generated by the windshield wipers is not transferred by car manufacturer C to the medium made accessible to B because C is afraid that this part of the data might disclose details about a new feature C is developing (activation of windshield wipers by the driver’s facial expression). Unless this was agreed between B and C, pruning the data by C would be in breach of the default terms incorporated under Principle 9(2)(a)(i).

55. Assume further that, in Illustration 53, a certain part of the data generated by the windshield wipers is made available to B only with a time lag of up to 30 minutes. Unless this was agreed between B and C, this deviation from real-time access would be inconsistent with the reasonable expectations of parties in a transaction of this kind and C would be in breach of the default terms incorporated under Principle 9(2)(a)(ii).

Another key difference between contracts for simple access to particular data under Principle 8 and contracts for exploitation of a data source under Principle 9 concerns terms as to the characteristics and quantity of data: Unless the parties have agreed otherwise, the supplier in a contract governed by this Principle has no obligation with respect to the quality or quantity of data to which the recipient will have access. Of course, parties will sometimes deviate from this default rule and agree, e.g., that the recipient will be enabled to harvest a particular minimum quantity of data and/or data of a particular minimum quality. But if both the quality and the quantity of data are clearly defined in the agreement, the transaction would often be one in which recipient is granted access to ‘particular data’ and the contract would be subject only to Principle 8. It is to be noted that the terms in Principle 8(2)(a)(i) and (ii) still apply and, thus, for example, material descriptions or representations would still be relevant.

Illustrations:

56. Assume that, in Illustration 51, business B approaches car manufacturer C, describes to C its plans to develop a smart weather report service for remote areas, and asks C whether there is any data generated by C’s cars that would be suitable for this purpose. C then offers to B access to the connected cars’ windshield wipers and headlights, to which B agrees. It turns out, however, that the headlights do not at all react to different weather conditions, but run in the same mode irrespective of whether rain is pouring or

1 the sun shining, and that the windshield wipers are automatically activated also where
2 there is dust on the windshield, rendering the windshield wiper data much less useful
3 for B’s purposes. As C had notice of B’s particular purpose for obtaining the data and
4 that B was relying on C’s skill or judgment in selecting the data source, the data source
5 must be fit for the recipient’s particular purposes. However, unless the parties have
6 agreed otherwise, B would not be entitled to a particular quantity of headlight or
7 windshield wiper data and, for example, B would not have any rights against C where
8 it turns out that buyers of C’s cars are becoming more and more climate-aware and use
9 their cars less and less often.

10 As to terms with regard to control or use of any data ported by the recipient in accordance
11 with the contract, the same default rules apply as under a contract for access to data under Principle
12 8.

13 **Illustration:**

14 57. In Illustration 52, company N would be under an obligation vis-à-vis B to seek valid
15 consent from the visitors to the website or to ensure otherwise that relevant data
16 privacy/data protection legislation is complied with. However, unless otherwise agreed
17 N would be under no obligation to B that there will be a particular number of clicks
18 from a particular number of visitors.

19 *c. Application of other law by analogy.* Contracts for the access to a data source do not
20 readily analogize to other well-developed sets of contract law rules. A functional analogy might be
21 that of a lease of the medium, device or facility to which the recipient is granted access, where the
22 recipient gets a significant degree of (temporary) control over that source. This device or facility is
23 often owned or otherwise run by the supplier, so if the supplier contracts for the use of that facility
24 by the recipient for the purpose of the collecting and further processing of data it is not far-fetched
25 to analyze this as a form of lease or a contract akin to lease. This analysis may be useful where, for
26 instance, a court needs to fill a gap in the contract.

27 **Illustration:**

28 58. In Illustration 52, company N enters into a contract with B to allow it to use the news
29 website, for a specified amount of time, for monitoring and recording the browsing

1 behavior of visitors. N's obligation vis-à-vis B to enable it to pursue its activities during
2 that time period could be analogized to the obligation of a lessor to enable a lessee to
3 use a leased facility. Accordingly, should B claim that it accessed the data only during
4 a small portion of that time and, thus, should not have to pay for the portion of the access
5 period that it did not utilize, that claim would not succeed, just as a lessee of a facility
6 must pay the full lease price without regard to how often it used the facility during the
7 term of the lease.

8 In jurisdictions where there is a difference between such lease contracts where the lessee is
9 allowed only to use the leased object, and lease contracts where the lessee may derive and keep the
10 fruits of the leased object (such as the crop yielded by a farm or the profit yielded by a restaurant)
11 the appropriate analogy would be rather the latter, depending on whether and to what extent the
12 recipient is allowed to port and keep data.

13 **REPORTERS' NOTES:**

14 **U.S.:**

15 As to the absence of a default term about the quantity of data that will be involved, an
16 analogy may be drawn between the sort of transactions covered by this Principle and output
17 contracts governed under the law of sales. See UCC § 2-306. See also Restatement (Second),
18 Contracts, Introductory Note to Chapter 11 (“The obligor who does not wish to undertake so
19 extensive an obligation may contract for a lesser one by using one of a variety of common clauses:
20 ... he may restrict his obligation to his output or requirements ...”).

21 As to the absence of a default term with respect to the quality of the data, an analogy may
22 be drawn to “as is” sales under UCC § 2-316, which contain no implied warranties. While an
23 explicit phrase such as “as is” can exclude such warranties under UCC § 2-316(3)(a), such
24 warranties may also be excluded by the commercial context as shown by course of dealing, course
25 of performance, or usage of trade. See UCC § 2-316(3)(c).

26 **Europe:**

27 It is typical for contracts for the lease of a particular device under the laws of the various
28 European jurisdictions that implied warranties refer to the item made available to the lessee, and
29 not to the benefits the lessee with ultimately derive from the leased item (see Section 1090 ff of the
30 Austrian Civil Code; Section 1719 ff of the French Code Civil; Section 535 ff of the German Civil
31 Code). Some jurisdictions stress objective standards for the conformity of the leased items, such as
32 Section 1720(1) of the French Code Civil stating that the lessor has to deliver the goods ‘in a good
33 state of repair in all respects’. Other jurisdictions refer to the ‘agreed use’ and focus more on
34 subjective standards (cf. Section 1096 of the Austrian Civil Code; Section 535(1) sentence 2 of the
35 German Civil Code). Other jurisdictions follow a mixed approach (cf. Section 592 of the Slovenian
36 LOA: ‘agreed or customary use’). In many jurisdictions, a difference is made between contracts
37 about items that are only for the lessee’s use (e.g. a residential apartment), and contracts about

1 items that are for economic exploitation by the lessee (e.g. a restaurant). In particular in the latter
2 case it is often difficult to draw a clear line between the features of the leased items, which are part
3 of the lessor's contractual obligations, and the lessee's expected benefit from the use, which is
4 entirely at the risk of the lessee.

5 **Principle 10: Contracts for authorization to access**

6 **(1) A contract for authorization to access data is one under which the supplier (referred to**
7 **in this Principle as the 'authorizing party') authorizes the access to data or a data source**
8 **by the recipient, including usually processing or porting of the data, but where, in the**
9 **light of the passive nature of the authorizing party's anticipated conduct under the**
10 **contract and the authorizing party's lack of meaningful influence on the transaction, the**
11 **authorizing party cannot reasonably be expected to undertake any responsibilities of the**
12 **sort described in Principles 7 to 9.**

13 **(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the**
14 **law should provide that in a contract for authorization to access:**

15 **(a) With regard to the mode of the recipient's access, a term that the authorizing party**
16 **will facilitate or assist the recipient in gaining access is not included, and the**
17 **authorizing party may continue using the data or data source in any way, even if**
18 **this impairs the recipient's access or even renders it impossible;**

19 **(b) With regard to the characteristics of the data, there is no requirement that the**
20 **recipient will receive data of a particular quality or quantity;**

21 **(c) With regard to control of the data and any other data activities the recipient may**
22 **engage in, the authorizing party has no obligation to ensure that the recipient will**
23 **have any particular rights;**

24 **(d) As between the authorizing party and the recipient, the recipient is responsible for**
25 **compliance with any duties vis-à-vis third parties under Part IV, including the**
26 **duties incumbent on a supplier of data under Principle 32; and**

27 **(e) The recipient must indemnify the authorizing party for any liability vis-à-vis third**
28 **parties that follows from the authorizing party's authorization to access the data**
29 **unless such liability could not reasonably be foreseen by the recipient.**

1 **(3) In determining which rules and principles to apply by way of analogy, as provided in**
2 **Principle 5, to contracts for authorization to access data, consideration should be given**
3 **to whether the focus of the agreement between the parties is on the access to the data or**
4 **on the supply of another commodity (such as a digital service) in the course of which**
5 **access to the data occurs.**

6 **Comment:** *a. Scope.* Principle 10 addresses data transactions in which the authorizing party
7 provides the recipient with access and allows processing but undertakes no obligations with respect
8 to that data. In contrast to a contract for access to particular data under Principle 8 or for access to
9 a data source under Principle 9, the authorizing party does not in any way undertake to support the
10 recipient in accessing or processing the data or to remove any technical or legal barriers.

11 *b. Default terms.* As set out in paragraph (2), the default terms in a contract for authorization
12 to access are rather minimal, putting no obligations on the authorizing party. In particular, subject
13 to contrary agreement of the parties as far as such contrary agreement is consistent with mandatory
14 law (see Principle 5), the supplier (who, in order to contrast the position of the parties in the
15 contracts governed by this Principle with those covered by Principles 7 to 9, is referred to as
16 ‘authorizing party’) does not undertake to facilitate or assist the recipient in gaining access. Also,
17 the authorizing party may continue using the data or data source (e.g., an electronic device) as the
18 authorizing party wishes, even if this impairs the recipient’s access or renders it impossible (e.g.,
19 because the device is disconnected from the Internet). Accordingly, the authorizing party does not
20 warrant that the recipient will receive data of a particular quality, fitness for purpose, or quantity,
21 nor that the recipient will have a particular legal position with regard to the data.

22 **Illustration:**

23 59. Provider M provides a messenger application and service ‘for free’. In return, users
24 authorize the processing of personal data on the device on which the application is
25 installed for a variety of purposes that are in M’s commercial interest. In this passive
26 access situation, the users are under no obligation actually to use the messenger service,
27 to produce a minimum quantity of user-generated data, or to produce data of a particular
28 quality (e.g. data that reveals the actual identity of the individuals with whom the users

1 correspond). Users are also free to delete the application, thus making any further access
2 to the data source on the part of M impossible.

3 *c. Duties with respect to third parties.* Unlike the contracts described in Principles 7 to 9
4 above, where the default terms primarily impose duties on the supplier, Principle 10 contains
5 default terms that impose significant duties on the recipient. If the authorizing party were to qualify
6 as a normal ‘supplier’, it would be subject both to any duties it owes vis-à-vis third parties under
7 Principle 32 and to potential liability where these duties are breached; but in a contract for
8 authorization to access, those costs should not ordinarily be borne by the authorizing party, whose
9 role is quite passive. Accordingly, Principle 10(2)(d) supplies a default term stating that the
10 recipient is, as between the authorizing party and the recipient, responsible for complying with the
11 duties under Principle 32. Also, under Principle 10(2)(d), the recipient must indemnify the
12 authorizing party for any liability vis-à-vis third parties that follows from authorization to
13 processing unless such liability was not reasonably foreseeable by the recipient.

14 **Illustration:**

15 60. Assuming that provider M in Illustration 59 not only instigates user C to permit
16 processing of C’s own personal data, but also to ‘authorize’ the processing of personal
17 data of all individuals displayed under C’s contacts on the mobile device. Even though
18 it is still primarily C who remains responsible vis-à-vis his friends, M has to assume
19 responsibility for making sure C is allowed to pass on his friends’ data and for
20 complying with all duties under Principle 32, and in case C is sued by one of his friends,
21 to indemnify C for all liability.

22 *d. Application of other law by analogy.* In deciding which law to apply by analogy within
23 the meaning of Principle 5, the focus of the parties’ agreement should be considered. In some
24 transactions, access to the data may be the main subject matter of the agreement. More often,
25 however, access to the data is not what the agreement, as reflected in the parties’ declarations and
26 any contract documents, is mainly about, but, rather, is an incidental element within a wider
27 transaction about something else, such as provision of some digital service (e.g. search engine
28 service, navigation service, messenger service) by the recipient of the data to whom authorization
29 to access is granted. Where this is the case, authorization to access is best seen not as the defining

1 characteristic of the transaction but, rather, as a substitute for payment in money for the digital
2 service.

3 **Illustrations:**

4 61. In Illustration 59, user C allows provider M to use C’s devices (e.g. a mobile phone
5 and messenger application) for the collection of personal data. A court might, where
6 relevant in a domestic legal system, analyze this as a case of consideration other than
7 money.

8 62. Farm corporation F buys a ‘smart’ tractor from seller S, which has been manufactured
9 by manufacturer T. The tractor comes with digital services, including weather forecasts,
10 soil analyses, targeted recommendations concerning the use of particular fertilizers and
11 insecticides, and predictive maintenance, to be provided by T and companies U and V
12 that cooperate with T. T, U and V will normally use the data that is collected by the
13 sensors of the tractor for their own commercial purposes. Economically speaking, T, U
14 and V will consider the value of the data they will probably receive, and the profits they
15 can derive from exploiting the data, when calculating the price to be charged for the
16 tractor and any digital service provided.

17 The insight that authorizing the processing of user-generated data amounts to a form of
18 payment, at least from an economic point of view, may be relevant in a number of different
19 contexts. *E.g.*, where a jurisdiction provides different rules for gratuitous contracts and for non-
20 gratuitous contracts, the fact that data is provided in lieu of a sum of money may mean that the
21 contract should be treated as a non-gratuitous contract.

22 **REPORTERS’ NOTES:**

23 **U.S.:**

24 As to the basic default terms, see Reporters’ Notes to Principles 7-9.

25 Some of the matters in this Principle are addressed from a different perspective in Principles
26 of the Law, Data Privacy, § 5. That section addresses the nature of the consent necessary on the
27 part of the authorizing party to enter into a transaction of this sort. The section requires that “When
28 consent is required, [the authorizing party] shall be given understandable and easy-to-use means to
29 permit exercise of meaningful choice in relation to personal data activities regarding the
30 [authorizing party’s] personal data.” *Id.* § 5(b). Further, the authorizing party must be provided
31 reasonable notice and consent may not be obtained in a misleading or deceptive fashion. *Id.* §§
32 5(e), 5(f). Additionally, the form by which consent is obtained must be reasonable under the

1 circumstances. Id. § 5(g)(1). Finally, the authorizing party may withdraw consent, subject to legal
2 or otherwise reasonable restrictions, by providing reasonable notice to the recipient. Id. § 5(h).

3 [Reporters' Note to be expanded in next draft.]

4 **Europe:**

5 *a. Scope.* In Europe, there is much awareness of the phenomenon of businesses collecting
6 data, in particular (but not exclusively) personal data, from their contracting partners for
7 commercial purposes. Often, but not always, this occurs in the context of a contract for digital
8 services that is purportedly provided 'for free', while really the business is providing the service in
9 return for the data collected. Recently, this phenomenon has spread far beyond 'pure' digital
10 services such as search engines, messenger services or social media, to the tangible world. E.g.,
11 many fleets of electrical scooters for hire in bigger cities are said to be run exclusively with the
12 purpose of collecting mobility and other relevant data, as it is clear from the outset that the rather
13 nominal monetary fees charged for hiring the scooter will suffice to amortize the purchase price
14 during the scooter's short lifespan. In legal terms, this phenomenon has been discussed as 'data as
15 counter-performance' or 'data as consideration'. It was first addressed openly by the European
16 legislator in the 2011 CESL Proposal, and later in the 2015 Proposal for a Directive on contracts
17 for the supply of digital content (COM(2015) 634 final). Article 3(1) of this Proposal had stated
18 that the proposed Directive should apply to any contract where the supplier supplies digital content
19 to a consumer and, in exchange, a price is to be paid 'or the consumer actively provides counter-
20 performance other than money in the form of personal data or any other data'. It was after the
21 European Data Protection Supervisor, in the famous Opinion No. 4/2017, had compared the
22 concept to trade in live human organs and stated that the catchphrase of 'paying with data' could
23 be dangerous if turned into a legal principle (No. 17 (with endnote 27) of EDPS Opinion 4/2017),
24 that the wording was changed. The final Digital Content and Services Directive (DCSD, Directive
25 (EU) 2019/770) now makes payment of a price or provision of data by the consumer beyond what
26 is necessary for the fulfilment of the contract or of legal duties an objective requirement for the
27 Directive's legal regime to apply, thus avoiding any explicit classification of data as 'counter-
28 performance', while the underlying idea remains the same (Article 3 DCSD). The notion has now
29 been extended to the Consumer Rights Directive (see Article 3(1a) of Directive 2011/83/EU, as
30 recently adapted by Directive (EU) 2019/2161). The immediate consequence is that a consumer
31 has the same rights (with regard to information, a right of withdrawal, or remedies for lack of
32 conformity) irrespective of whether a price is paid in money or whether data is provided.

33 *b. Default terms, c. Duties with respect to third parties and d. Application of other law by*
34 *analogy.* Before the wording was changed and while data was still explicitly qualified as 'counter-
35 performance' there had been a lively academic debate concerning the consumer's duties and
36 potential liability for breach, e.g. if the consumer withdraws their consent to the processing of
37 personal data, or provides poor data quality (such as a fake name), or fails to make sure other
38 affected individuals have given consent to the processing of their data (see Axel Metzger, Data as
39 Counter-Performance – What Rights and Duties do Parties Have?, JIPITEC 2017, 6). While the
40 academic debate is still ongoing it has arguably been overtaken by developments. Given that the
41 European legislator clearly changed its strategy and no longer qualifies data as 'counter-
42 performance' or 'consideration' but rather insists that data protection is an inalienable human right,
43 any liability of the consumer for breach, or even more so an enforceable obligation to provide data,
44 should be definitely off the table. However, the DCSD leaves it a matter of national law to set out
45 the consequences for the contract in the event that the consumer withdraws the consent for the

1 processing of the consumer's personal data (Recital 40 DCSD). In all events national law can only
2 provide for consequences that are consistent with the GDPR.

3 **Principle 11: Contracts for data pooling**

4 **(1) A contract for data pooling is one under which two or more parties (the ‘data partners’)**
5 **undertake to share data in a data pool by**

6 **(a) transferring particular data to a medium that is jointly controlled by the data**
7 **partners or that is controlled by a data trustee or escrowee or other third party**
8 **acting on behalf of the data partners; or**

9 **(b) granting each other access to particular data or the possibility to exploit particular**
10 **data sources, with or without the involvement of a third party.**

11 **(2) This Principle applies, with appropriate adjustments, to the governing principles of any**
12 **entity created pursuant to a data pooling contract.**

13 **(3) Subject to agreement of the parties and to rules that take priority pursuant to Principle**
14 **5, the law should provide that the following terms are included in a contract for data**
15 **pooling:**

16 **(a) A data partner may utilize data from the data pool, or data derived from such data,**
17 **only**

18 **(i) for purposes agreed upon between the data partners in the contract for data**
19 **pooling;**

20 **(ii) for purposes which the relevant data partner could reasonably expect to be**
21 **accepted by the other data partners, unless these purposes are inconsistent**
22 **with an agreement referred to in subparagraph (i); or**

23 **(iii) as necessary to comply with applicable law;**

24 **(b) A data partner may engage data processors, but may otherwise pass data from the**
25 **data pool, or data derived from such data, on to third parties only under the**
26 **conditions agreed upon between the data partners or required by applicable law;**

1 **(c) As between the data partners, new intellectual property rights or similar rights**
2 **created with the use of data from the data pool belong to the partner or partners**
3 **who conducted the activity leading to the creation of the new right;**

4 **(d) If a data partner leaves the data pool, the data supplied by that data partner must**
5 **be returned to the relevant data partner, but data derived from the data, unless**
6 **essentially identical with the original data, remains in the pool. Upon leaving the**
7 **data pool, a data partner is entitled to a copy of any data in the pool that has been**
8 **derived, in whole or in substantial part, from data supplied by that data partner.**

9 **(4) In determining which rules and principles to apply by way of analogy, as provided in**
10 **Principle 5, to contracts for data pooling, consideration should be given to whether the**
11 **relationship between the data partners is one characterized by mutual trust and**
12 **confidence, such that the data partners owe each other fiduciary obligations, or, rather,**
13 **whether it is characterized by arm's length transactions with no fiduciary obligations.**

14 **Comment:** *a. Scope.* Principle 11 applies to a phenomenon under which separate parties,
15 which are here called the ‘data partners’, agree to share data in a way that there is not a ‘supplier’
16 and a ‘recipient’ but that each of the parties is, at the same time, both supplier and recipient with
17 regard to data shared in a data pool. Often, such arrangements are referred to as ‘closed data
18 platforms’, with ‘closed’ indicating that the data pool is accessible only to the data partners
19 involved and not to a wider public, such as under open data schemes. The technical and legal
20 arrangements in place may vary. Very often, the data partners will transfer data to a medium (or a
21 defined sector of such a medium, such as cloud space) that is controlled jointly by all partners or
22 by a third party. The third party may, in particular, be a data trustee within the meaning of Principle
23 13, or an escrowee within the meaning of Principle 14, or a new company established and held
24 jointly by the data partners specifically for the purpose of managing and exploiting the data pool.
25 But it is also possible that the data pool is held in a decentralized manner on media controlled by
26 each of the data partners, who then give access to that data to the other data partners within the
27 meaning of Principle 8. Often, the data partners will focus on the exploitation of particular data
28 sources within the meaning of Principle 9 rather than on particular data. All these arrangements
29 may be qualified as contracts for data pooling.

1 **Illustration:**

2 63. Tractor manufacturers M, N and O agree to pool, and therefore to grant each other
3 access to, a particular type of data generated by their respective smart tractors with the
4 aim of better enabling each of them to provide a smart service, such as recommendations
5 as to optimal use of insecticides, to farmers. If M, N and O transfer particular data sets
6 from the past to a server controlled jointly by M, N and O, this is a contract for data
7 pooling based on data transfer (Principle 7). If M, N and O provide each other with
8 access credentials to particular data sets stored on their respective servers, this is a
9 contract for data pooling based on data access (Principle 8). If M, N and O promise each
10 other access to all the data produced by their fleet of tractors, which will be transferred
11 in real time to a server controlled jointly by M, N and O, this is a contract for data
12 pooling based on exploitation of data sources (Principle 9).

13 *b. Default terms.* As with other contracts addressed in this Chapter, parties to contracts for
14 data pooling will likely negotiate and draft contractual language to cover important business terms,
15 but it may still be essential to determine the parties' rights and responsibilities with respect to
16 matters that were not the subject of explicit agreement. Paragraphs (3) and (4) of this Principle
17 address some of these issues.

18 The application of paragraph (3) depends on which of the three types of data pooling
19 contract is present. In cases in which the contract provides for the transfer of data to a closed
20 platform that is jointly controlled by the data partners or that is controlled by a third party acting
21 on behalf of the data partners, the default rules in Principle 7 are applicable. In cases in which the
22 contract provides for the parties granting each other access to the data, the default rules in Principle
23 8 are applicable. Finally, in cases in which the contract provides for the parties granting each other
24 the right to exploit particular data sources, the default rules in Principle 9 are applicable. In addition
25 to incorporating default rules from Principles 7 to 9, paragraph (3) adds five more default rules.

26 First, in contrast with the 'sales' approach chosen by Principle 7 and, as far as data rightfully
27 ported are concerned, by Principles 8 and 9, Principle 11 opts for a 'license' approach. This means
28 that a data partner may utilize data from the data pool only for the purposes agreed upon between
29 the data partners or required by law. As the parties may not be able to think of all eventualities,
30 paragraph 3(a) clarifies that a data partner may also use data from the data pool for purposes that
31 data partner could reasonably expect to be accepted by all the other data partners.

1 **Illustration:**

2 64. Assume that M, N and O in Illustration no. 63 agree that the pooled tractor data may
3 be used for improving the data bases for an enumerative list of precision farming
4 services. N decides to engage also in real estate services, arranging deals between
5 buyers and sellers of farmland and providing services in this context. Without an
6 additional agreement between M, N and O to that end, N would not be allowed to use
7 data from the data pool (other than the data N itself contributed) for this new purpose.
8 N would not be able to rely on a reasonable expectation that the other partners would
9 accept this, as it significantly enhances the data pool's utility for N, at the expense of
10 M and O, which might have had similar plans, or might even get into trouble with the
11 farmers using their tractors. Where, on the other hand, N wishes to report on the new
12 data pool at its annual shareholder meeting and to show some slides with statistical data
13 derived from the data in the pool, and the data does not disclose anyone's business
14 secrets, N could reasonably expect that this would be accepted by M and O.

15 Second, in line with this 'license approach' paragraph (3)(b) states that a data partner may
16 engage data processors, but may otherwise pass data from the data pool, or data derived from such
17 data, on to third parties only under the conditions agreed upon between the data partners or
18 mandated by law. After all, it can be expected that the data partners are agreeing to share among
19 themselves and would want the right to prevent others who are not parties to the contract from
20 obtaining access to the data.

21 Third, the default rules in paragraph (3)(c) address the topic of ownership of new
22 intellectual property rights or similar rights created with use of the shared data. Paragraph (3)(c)
23 provides, as a default rule, that new intellectual property rights or similar rights created with the
24 use of data retrieved from the platform shall belong, as between the data partners, to the partner or
25 partners who conducted the activity leading to the creation of the new right. With this as a default
26 rule, the parties will have an incentive to bargain explicitly if they want a different allocation of
27 such new rights. While paragraph (3)(c) provides a default rule for ownership of those new rights,
28 it should be noted that applicable intellectual property law might require the parties to execute an
29 instrument transferring those rights from whoever would own them under that law to those who
30 are to own them under the contract.

1 **Illustration:**

2 65. Assume that N and O in Illustration no. 63, with the help of data from the pool and in
3 line with the purposes agreed upon between all three partners, develop, with the help of
4 their respective R&D departments, a new smart service with significantly more granular
5 recommendations as to the type and optimal amount of insecticides required. As
6 between the three data partners, the intellectual property rights in this new smart service
7 (the type of which, such as copyright or a patent right, would depend on the applicable
8 intellectual property regime) would belong to N and O, who have invested in the
9 development of the new service, unless M, N, and O have agreed otherwise. If the
10 applicable intellectual property regime assigns rights in a different manner, there would,
11 by default, be a contractual obligation to bring the situation, as between the data
12 partners, into line with paragraph (3)(c).

13 Fourth, paragraph (3)(d) together with Principle 4(2) and (3) provides that if a data partner
14 leaves the data pool, the data supplied by that data partner must be erased or, where erasure of the
15 data would be unreasonable under the circumstances within the meaning of Principle 4(3), an
16 allowance be made in money. Upon leaving the data pool, a data partner is entitled to a copy of
17 any data in the pool that has been derived, in whole or to a substantial part, from data supplied by
18 that data partner. (Naturally, where the whole data pooling contract is terminated and all data
19 partners leave the pool, this applies to all of the partners.).

20 **Illustration:**

21 66. Assume that O in Illustration no. 63 decides to leave the data pooling contract, which
22 is silent as to the further destiny of the data. In this case, paragraph (3)(d) provides that
23 the data generated by all smart tractors produced by O must be returned to O and must
24 be erased from the pool. Where data has been derived from that data, and the derived
25 data is not essentially identical with the data contributed by O (such as in Illustration
26 no. 65 where O's data has been aggregated with N's data to create added value) the
27 derived data may remain in the pool, but O is entitled to a copy.

28 *c. Application of other law by analogy.* When deciding which other law to apply—either
29 directly or by analogy—the first question that needs to be asked is whether or not a company under
30 company law has been established, in which case many issues, such as the contributions to be made

1 by the partners, and the benefits to be derived by the partners, would be regulated directly by
2 company law. Generally speaking, consideration should be given to whether the relationship
3 between the data partners is one characterized by mutual trust and confidence, such that the data
4 partners owe each other fiduciary obligations, or, rather, whether it is characterized by arm's length
5 transactions with no fiduciary obligations.

6 REPORTERS' NOTES:

7 U.S.:

8 Data pools can be further divided into public data pools and private data pools. “Public data
9 pools co-mingle data assets from multiple data holders—including companies—and make those
10 shared assets available on the web. Pools often limit contributions to approved partners (as public
11 data pools are not crowdsourcing efforts), but access to the shared assets is open, enabling
12 independent uses. Nonetheless, the pools are usually developed primarily to provide utility to
13 contributing partners or other user groups such as medical researchers or humanitarian actors.”
14 Stefaan G. Verhulst, Andrew Young, Michelle Winowatan, and Andrew J. Zahuranec, *Leveraging
15 Private Data for Public Good: A Descriptive Analysis and Typology of Existing Practices* at 24
16 (Govlab 2019), available at <https://datacollaboratives.org/static/files/existing-practices-report.pdf>.

17
18 By way of contrast, in private data pools “Partners from different sectors pool data assets
19 in a controlled and restricted access environment. Unlike public data pools, this approach limits
20 data contribution and data access to only approved partners. Private data pools tend to be highly
21 topic-specific with development and maintenance aimed at serving a particular user group.” *Id.* at
22 26.

23 Europe:

24 *a. Scope.* In Europe, data pooling arrangements are usually treated as a form of ‘data
25 sharing’ (cf. Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, ‘Competition
26 policy for the digital era’, 2019, p. 9). Compared with other data sharing arrangements, the
27 distinctive feature of data pooling is that there is not one party who is the supplier and one party
28 who is the recipient, but instead each party is both supplier and recipient at the same time. There is
29 no generally recognised terminology for such arrangements, and they may equally be described,
30 e.g., as ‘closed platform’ or ‘data-sharing partnership’, but they are definitely rather common (cf.
31 OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use
32 across Societies*, 2018, p. 46 f.). Some authors have defined data pooling as an agreement whereby
33 companies share data ‘in reference to a given service or generally in an industry, or within an e-
34 ecosystem’ (see Björn Lundqvist, *Competition and Data Pools*, (2018) *Journal of European
35 Consumer and Market Law* 4, p. 146; Heiko Richter and Peter R. Slowinski, *The Data Sharing
36 Economy: On the Emergence of New Intermediaries*, (2019) *International Review of Intellectual
37 Property and Competition Law* 50, p. 4, 11). The European Commission has described ‘data
38 exchange in a closed platform’, set up either by one core player in a data sharing environment or
39 by an independent intermediary, as one of the standard forms of B2B data sharing (see *Guidance
40 on sharing private sector data in the European data economy*, accompanying the document
41 *Communication from the Commission to the European Parliament, the Council, the European*

1 Economic and Social Committee and the Committee of the Regions ‘Towards a common European
2 data space’, SWD(2018) 125 final, p. 5).

3 *b. Default terms and c. Application of other law by analogy.* Since the datasets in a data
4 pool are digital assets that come from different data partners and are used – at least to some extent
5 – with a common interest, similarities can be drawn to the assets of a company (partnership).
6 Comparable provisions to default rules set out by Principle 11 can therefore be found in European
7 company law. Comparable to Principle 11(2)(a) and (b), national laws limit the use of company
8 assets by individual partners. For example, the partner of a German General Partnership may not
9 dispose of their share of the company's assets and of the individual items belonging thereto (§ 719
10 BGB). For Austrian General Partnerships, Section 122(2) of the Commercial Code (UGB) provides
11 that a partner may not withdraw company assets without the consent of the other partners.

12 National provisions on the retirement from and the dissolution of partnerships have inspired
13 the default rule, that a partner leaving the data pool should be returned any data that had been
14 supplied. For example, the German Civil Code lays down stipulates that all objects which the
15 withdrawing partner has left to the partnership shall be returned (§ 738 BGB). A similar default
16 rule can be found in the Austrian Commercial Code (see § 137(1) UGB). In France, Article 1844-
17 9 Code Civil provides that after payment of the debts and repayment of the share capital, the
18 division of the assets is carried out between the partners in the same proportions as their
19 participation in the profits, unless otherwise stipulated or agreed.

20 Chapter C: Contracts for Services with regard to Data

21 Principle 12: Contracts for the processing of data

22 **(1) A contract for the processing of data is one under which a processor undertakes to**
23 **process data on behalf of the controller. Such processing may include, inter alia:**

24 **(a) the collection and recording of data (e.g., data scraping);**

25 **(b) storage or retrieval of data (e.g., cloud space provision);**

26 **(c) analysis of data (e.g., data analytics services);**

27 **(d) organization, structuring, presentation, alteration or combination of data (e.g., data**
28 **management services); or**

29 **(e) erasure of data.**

30 **(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the**
31 **law should provide that the following terms are included in a contract for the processing**
32 **of data:**

- 1 **(a) The processor must follow the controller’s directions and act consistently with the**
2 **controller’s stated purposes for the processing;**
- 3 **(b) The processor must ensure at least the same level of data security and of protection**
4 **for the rights of third parties as the controller was under an obligation to ensure,**
5 **and must support the controller in complying with any legal obligations for the**
6 **protection of third parties that could reasonably be expected in a situation of the**
7 **relevant kind or of which the processor had notice when the contract was made;**
- 8 **(c) The processor must not pass the data on to third parties;**
- 9 **(d) The processor may not process the data for the processor’s own purposes, except to**
10 **the extent reasonably necessary to improve the quality or efficiency of the relevant**
11 **service, so long as this does not harm the controller’s legitimate interests and is not**
12 **inconsistent with obligations for the protection of third parties within the meaning**
13 **of paragraph (2)(b); and**
- 14 **(e) Upon full performance or termination of the contract, the processor must transfer**
15 **to the controller any data resulting from the processing that has not already been**
16 **transferred. The processor must subsequently erase any data retained, except to the**
17 **extent reasonably necessary for existing or likely litigation or to the extent that the**
18 **processor has a legal right or obligation independent of these Principles to keep the**
19 **data beyond that time.**
- 20 **(3) In determining which rules and principles to apply directly or by way of analogy, as**
21 **provided in Principle 5, to contracts for processing of data, consideration should be**
22 **given to the nature of the service, such as to whether the focus is on changing the data**
23 **or on keeping it safe.**

24 **Comment:** *a. Scope.* Contracts for the processing of data, as described in paragraph (1), are
25 common. Given the broad definition of ‘processing’ under Principle 3(1)(c), these contracts may
26 appear in an extremely broad variety of forms. Contracts for processing of data may relate to the
27 collection and recording of data (e.g. data scraping), to its storage or retrieval (e.g. cloud space
28 provision), to its organisation, structuring, presentation, alteration or combination (e.g. data
29 management services), to analysis of it (e.g. data analytics services), or to its erasure.

1 **Illustration:**

2 67. Real property business C hires the services of company P to create digital twins of C's
3 buildings for facilitating maintenance. This includes the processing of a broad range of
4 data, including data collected by a variety of sensors in the buildings and photographic
5 data collected by drones. In this situation, C defines the means and purposes of the
6 collecting and other processing of the data and P's motivation for processing the data is
7 to fulfill its contract with C, so C is the controller, and P qualifies as processor and the
8 contract is one for the processing of data within the meaning of Principle 12.

9 The description of 'contract for processing', in Principle 12(1) should be read in
10 conjunction with the limitation in Principle 2(1) to matters for which 'the primary focus of the
11 matter is on records of large quantities of information as an asset, resource or tradeable
12 commodity.' Accordingly, although Principle 12(1) could be read in isolation as covering some
13 contracts involving the processing of data but where the focus of the transaction is not related to
14 these Principles (e.g. a photographer's services, proofreading a manuscript, etc.), such contracts
15 are not within the scope of Principle 12.

16 In the light of the broad definition of 'processing' under Principle 3(1)(c), situations where
17 a contracting partner engages in processing activities while fulfilling contractual duties will be
18 common even within the general scope of the Principles. However, Principle 12 should apply only
19 where the focus of the agreement is on the processing activities as such, not where processing is
20 necessary merely to fulfill an obligation of a different nature. For example, where the operator of
21 a data marketplace contract within the meaning of Principle 15, in order to fulfil its obligations
22 under the data marketplace contract by facilitating a transaction between the client and other
23 parties, processes some data provided by the client (e.g. in order to transfer it to the client's
24 contracting party), this still should be treated as a contract under Principle 15, and not under
25 Principle 12; however, as far as the processing activities are concerned, the default terms under
26 Principle 12 might still prove to be useful. Where, on the other hand, data storage and storage
27 management are important aspects of the contractual obligations of a data trustee within the
28 meaning of Principle 13, it may be justified to apply both Principles 12 and 13 for the respective
29 aspects of the bundle of obligations.

1 *b. Default terms applicable to contracts for processing of data.* Paragraph 2(a) is
2 straightforward – a contract for the processing of data has, as a default term, an obligation of the
3 processor both to follow the controller’s directions and to act consistently with the controller’s
4 stated purposes for the processing.

5 **Illustration:**

6 68. If, in a situation such as the one in Illustration no. 67, real property business C directs
7 company P not to create a digital twin of a particular building (e.g. because of security
8 concerns raised by a State authority that is a tenant in that building), P must comply
9 with that direction, even if there is no explicit clause to that end in the contract. Whether
10 or not P has a claim to be paid for creating a digital twin of that building, if the building
11 was included in the initial contract, is a different question and depends on the applicable
12 contract law.

13 In the event of a conflict, the controller’s directions typically should prevail, but where the
14 processor is more sophisticated and realizes that the controller’s directions are inconsistent with
15 the purpose the processor may reasonably be expected to notify the controller.

16 Under paragraph 2(b), the processor has a duty to provide the same level of data protection
17 and data security for protecting the rights of third parties as the controller is under an obligation to
18 ensure, and similarly must support the controller in complying with its legal obligations in this
19 regard. Generally, these duties are present only if such obligations could reasonably be expected in
20 a situation of the relevant kind or if the processor had notice of the controller’s obligations.

21 **Illustration:**

22 69. Assume that C in Illustration no. 67 may create a digital twin of all buildings, but is
23 under an obligation vis-à-vis a State authority that is a tenant of one of C’s buildings to
24 treat any data of that building with a particular degree of data security. If P has notice
25 of these requirements when the contract is made, or if the requirements could reasonably
26 be expected, P is under an obligation to apply the same level of security to the data
27 produced.

28 Paragraph (2)(c) provides that the processor must not pass data on to third parties because
29 such action by the processor may harm the legitimate interests of one or both the controller and

1 third parties to whom the controller is responsible. There may, of course, be situations where the
2 processor has a legitimate interest in passing on data, e.g. where the processor needs to engage a
3 subcontractor. However, because paragraph 2(c) is only a default term, the processor and controller
4 are free to agree on appropriate conditions for the engagement and duties of a subcontractor.

5 **Illustration:**

6 70. In the situation described in Illustration no. 69, P may require the services of
7 independent company P to produce the digital twins. If this is the case, P must raise this
8 point in the negotiations with C. P would need to procure C's agreement to the use of
9 the independent company as a subcontractor. C and P might agree, for example, that the
10 subcontractor is allowed so long as the same level of protection is ensured, plus that P
11 remains fully responsible for what the subcontractor does.

12 Paragraph (2)(d) provides that the processor must refrain from any processing of the data
13 for the processor's own purposes. This should not be interpreted as implying that the experience
14 gained by the processor cannot benefit the processor in subsequent contracts. For instance, where
15 the processor, in the course of fulfilling its duties under the contract for processing with the
16 controller, uses AI, and that AI improves by being run on the controller's data, the processor may
17 of course keep the improved AI and may benefit from that when dealing with the next customer.
18 As this is merely an incidental effect of fulfilling the contract with the controller and does not harm
19 the controller's interests it is not prohibited by the default term under (2)(d). This is why (2)(d)
20 contains an exception where use of the data is reasonably necessary to improve the quality or
21 efficiency of the relevant service, so long as this does not harm the controller's legitimate interests
22 and is not inconsistent with any of the controller's legal obligations for the protection of third
23 parties that could reasonably be expected in a situation of the relevant kind or of which the
24 processor had notice when the contract was made.

25 **Illustration:**

26 71. Assume that P in Illustration no. 67 wants to process the data produced for C in two
27 additional ways on which the contract document is silent: (a) analyzing it immediately
28 for internal quality control and optimization of drone trajectories while the contract is
29 still being performed, using only data that has been aggregated with data of other
30 controllers, rendering it unattributable to the controller; and (b) retaining the data in a

1 form that is still attributable to C to promote P’s services. Use of the data in the first
2 way is permitted by this default term because it is for the benefit of C and cannot harm
3 C’s interests, while use of the data in the second way would not be permitted by this
4 default term because it is inconsistent with C’s legitimate interest.

5 Paragraph (2)(e) addresses situations that may differentiate a contract for the processing of
6 data from other service contracts. While a service provider who undertakes to apply fresh paint to
7 a house, or to repair a car, or to transport goods from one place to another, has little opportunity to
8 retain the materials provided by the other party after the contract has been performed, the situation
9 is different with respect to data. In a contract for the processing of data, the processor would easily
10 be able to retain a copy of the data without the controller’s knowledge and at low cost for storage,
11 etc., creating a temptation to use the data for a separate commercial purpose of the processor.
12 Accordingly, paragraph 2(e) supplies a default term of the contract to the effect that the processor
13 must erase any data retained by the processor after the contract has been performed and the
14 processed data has been provided to the controller. There may be some circumstances, however,
15 where retention of a copy of the data for a short period of time after the contract has been performed
16 is not improper and is justified, e.g., by the processor’s interest in defending itself in pending or
17 imminent litigation. Even in those circumstances, however, retention of a copy would be a breach
18 of the supplier’s obligation if the terms of the contract indicate that retention of a copy is not
19 allowed for this purpose (subject to rules of law that cannot be derogated from by agreement, such
20 as doctrines of unconscionability).

21 **Illustration:**

22 72. Company P in Illustration no. 67 retains the data on its servers after having finished its
23 service for C. Retaining the controller’s data is normally not in conformity with the
24 terms of the contract. However, where C has already announced it will withhold
25 payment because the photographic material was not in conformity with the contract, P
26 may have a legitimate interest in retaining the material in order to use it in potential
27 litigation.

28 Under law governing the litigation process a party may have a duty to preserve copies, in
29 which case such a mandatory rule would govern.

1 Principle 12(2)(a). Clause 8 Module Two 8.1(a) of the SCC also sets out that the importer (i.e.
2 processor) agrees and warrants to process the personal data only on documented instructions from
3 the data exporter. Under a ‘traditional’ service contract, the service provider is – similar to Principle
4 12(2)(a) – generally obligated to follow directions of the client regarding the performance of the
5 service. However, these directions must be timely, and be part of the contract itself or specified in
6 a document to which the contract refers; result from the realization of choices left to the client by
7 the contract; or result from the realization of choices initially left open by the parties (see Article
8 IV.C. – 2:107(1) DCFR). If the direction bears the risk that the result stated or envisaged by the
9 client will not be achieved, or may damage other interests of the client, the service provider must
10 warn the client (Article IV.C. – 2:107(2) and Article IV.C. – 2:108(1) DCFR).

11 An obligation comparable to Principle 12(2)(b) can be found in Article 28(1) GDPR, which
12 requires the controller to only use processors who provide sufficient guarantees to implement
13 appropriate technical and organisational measures in such a manner that processing will meet the
14 requirements of the GDPR and ensure the protection of the data subject’s rights. There is also a
15 resemblance between Clause 8 Module Two 8.6(a) of the SCC and Principle 12(b). Pursuant to
16 Clause 8 Module Two 8.6(a), the importer shall implement appropriate technical and organizational
17 security measures to ensure the security of the data. Further, the duties in default rules (b) to (d)
18 draw clear inspiration from the duties of a storer in a storage contract, which is a special form of a
19 service contract, under which the storer is obligated to take reasonable precautions in order to
20 prevent unnecessary deterioration, decay or depreciation of the object stored (Article IV.C. –
21 5:103(1) DCFR). In addition, the storer may use the object entrusted for storage only if the client
22 has agreed to such use (Article IV.C. – 5:103(2) DCFR).

23 Article 28(3)(g) GDPR stipulates that the processor shall delete or return all the personal
24 data to the controller after the end of the provision of services relating to processing and delete
25 existing copies unless Union or Member State law requires storage of the personal data, which
26 corresponds to Principle 12(2)(e) (as well as to Principle 15(2)(d)). Similar provisions can be found
27 in other parts of the GDPR, e.g. in Article 17 GDPR on erasure of the data and also in Article 16(3)
28 Digital Content and Services Directive (DCSD, Directive (EU) 2019/770), according to which,
29 upon termination of the contract, the trader shall refrain from further use of content provided by
30 the consumer under the contract. Also under Clause 16(d) of the SCC the data that has been
31 transferred prior to the termination of the contract shall immediately be returned to the data exporter
32 or deleted in its entirety. The same shall apply to any copies of the data. Similarly, a storer in a
33 storage contract must return the object at the agreed time or, where the contractual relationship is
34 terminated before the agreed time, within a reasonable time after being so requested by the client
35 (Article IV.C. – 5:104(1) DCFR), which is also set out for the data resulting from the processing
36 that has not already been transferred in Principle 12(2)(e).

37 *c. Rules applicable to contracts for processing of data.* Under national legal systems, data
38 processing contracts will normally be qualified as contracts for service. At its core, service
39 contracts are understood as the supply of a service in exchange for remuneration. However, there
40 are differences in European legal systems as to the exact definition of service contract. Some
41 jurisdictions have different rules for material and intellectual services, while others apply the same
42 provision for all services other than storage. While all legal systems in the EU have specific rules
43 on storage contracts, their application usually requires that a tangible good is stored. Thus, in most
44 legal systems, the provisions for contracts for service also apply to cloud storage contracts. An
45 exception in this regard is Germany, where cloud computing contracts are generally classified as
46 lease/rental agreements that may have certain elements of a service contract

1 In English law, contracts for services are defined very broadly as ‘any contract under which
2 a person agrees to carry out a service’ in Section 12(1) of the Supply of Goods and Services Act
3 1982. Hence, the range of activities covered by this definition is very wide and covers both material
4 and intellectual services. Explicitly excluded from the statutory definition are contracts of service
5 (employment contracts) and contracts of apprenticeship. According to Section 12(3), a contract
6 does not fall outside the definition of a contract for services merely because goods are transferred
7 or bailed by way of hire. This broad definition is likely to cover most data processing contracts.

8 In France, the concept of ‘louage d’ouvrage’ (also: contrat de prestation de service) is very
9 broad in the sense that it covers any contract whereby one party agrees to perform work for another
10 party on an independent basis. The contract does not only include services relating to immovable
11 and movable objects but, according to a decision of the French Cour de Cassation, also covers
12 intellectual services (Cass. civ. III, 28 February 1984, Bull.civ. III, no. 51). Therefore, the general
13 provisions on louage d’ouvrage (cf. Articles 1710, 1779 and 1787 ff. of the French Civil Code)
14 also apply to the contracts referred to by Principle 12.

15 The German Civil Code distinguishes between ‘Werkvertrag’ (where the service provider
16 undertakes to achieve a particular result) and ‘Dienstvertrag’ (where the service provider only
17 promises best efforts). The concept of Werkvertrag, which is laid down in Sections 631 ff., is
18 considered to cover all kind of services and applies to services related to immovables and movables,
19 but also to intellectual services (cf. Section 631 (1)) and is thus likely to cover also most data
20 processing contracts. However, Dienstvertrag (Sections 611 ff.) may also cover a wide range of
21 different types of data processing services that would be covered by Principle 12. Some services
22 covered by Principle 12, such as contracts for the storage of data in a cloud, would be qualified in
23 a different manner, e.g. as lease (rental) contracts (Sections 535 ff., 578b).

24 **Principle 13: Data trust contracts**

25 **(1) A data trust contract is a contract among one or more controllers of data (the**
26 **‘entrusters’) and a third party under which the entrusters empower the third party (the**
27 **‘data trustee’) to make certain decisions about use or onward supply of data (the**
28 **‘entrusted data’) on their behalf, in the furtherance of stated purposes that may benefit**
29 **the entrusters or a wider group of stakeholders (such entrusters or stakeholders being**
30 **referred to as the ‘beneficiaries’).**

31 **(2) A data trust contract and the relationships it creates need not conform to any particular**
32 **organizational structure and need not include the characteristics and duties associated**
33 **with a common law trust. This Principle applies, with appropriate adjustments, to the**
34 **governing principles of any entity created pursuant to a data trust contract.**

35 **(3) Subject to agreement of the parties and to rules that take priority under Principle 5, the**
36 **law should provide that the following terms are included in a data trust contract or are**

- 1 **incorporated into the governing principles of any entity created pursuant to the data**
2 **trust contract:**
- 3 **(a) The data trustee is, subject to subparagraphs (b) and (c), empowered to make and**
4 **implement all decisions with regard to use or onward supply of the entrusted data,**
5 **including decisions concerning intellectual property rights and rights based on data**
6 **privacy/data protection law;**
- 7 **(b) The data trustee must act in furtherance of the stated purposes of the data trust**
8 **contract for the benefit of the beneficiaries and, even if the entrusters are not the**
9 **beneficiaries, in a manner that is not inconsistent with the legitimate interests of the**
10 **entrusters of which the data trustee has notice;**
- 11 **(c) The data trustee must follow any directions given by the entrusters, except to the**
12 **extent that the data trustee has notice that the directions are incompatible with the**
13 **stated or manifestly obvious purposes of the data trust;**
- 14 **(d) The data trustee must refrain from any use of the entrusted data for its own**
15 **purposes and must avoid any conflict-of-interest;**
- 16 **(e) The entrusters may terminate the data trustee’s power with regard to the data**
17 **entrusted by them at any time; however, this right may be limited to the extent**
18 **necessary to take into account reliance and similar legitimate interests of the**
19 **beneficiaries; and**
- 20 **(f) If the data trustee has retained any data entrusted, or any data derived from such**
21 **data, after the contract has come to an end (by termination or otherwise) the data**
22 **trustee must return the data to the entrusters, and, when reasonable, take steps to**
23 **prevent further use of the data by onward recipients.**
- 24 **(4) In determining which rules and principles to apply by way of analogy, as provided in**
25 **Principle 5, to data trust contracts, consideration should be given in particular to**
- 26 **(a) the stated purposes of the data trust contract and the nature of the data and of the**
27 **parties involved;**
- 28 **(b) whether the purposes of the data trust contract are primarily for the benefit of the**
29 **entrusters or broader constituencies; and**

1 **(c) the organizational structure of the relationships created by the data trust contract.**

2 **Comment:** *a. Scope.* This Principle provides a general overview of the legal principles
3 recommended for data trust contracts. As noted in paragraph (2), notwithstanding the use of the
4 term ‘trust’ in the nomenclature describing these arrangements, the arrangements need not include
5 the characteristics and duties associated with a common law trust. Principle 13 is stated at a high
6 level of generality because both the subject of data trust arrangements and the nature of those
7 arrangements can vary widely. Moreover, data trust arrangements are an emerging concept, with
8 new subjects and mechanisms constantly arising. The purpose of this Principle, as of most other
9 Principles, is facilitative. Thus, the description of types of data trust contracts, and the
10 recommended rules to govern them, are not limited to arrangements that are common today; rather,
11 they are designed to be flexible enough to accommodate arrangements that may emerge in the
12 future.

13 Data trust arrangements within the meaning of Principle 13 are often combined with
14 arrangements for the processing of data within the meaning of Principle 12, as the data trustee’s
15 activities under the data trust arrangements would often include storage of data and similar data
16 processing activities. When this is the case, both Principles 12 and 13 would apply, with Principle
17 13 more specifically dealing with the power of decision making, i.e. a power that rests with the
18 controller of data, and not with the processor. A data trustee is thus a person to whom one or more
19 controllers of data delegate (some of) their powers as controllers, while possibly engaging the same
20 party to provide other services under Principle 12.

21 Data trust arrangements are typically contracts that create a continuing relationship of a
22 particular or indefinite duration. While, theoretically, any contract dealt with under these Principles
23 could be either a one-time exchange or a continuing relationship, the contracts dealt with under
24 Principle 13, as well as some other Principles, are more often entered into for a particular or
25 indefinite period of time.

26 *b. Typical data trust arrangements.* Under this Principle, a wide variety of arrangements
27 may be governed as data trust contracts. All that is needed is a contract of the sort described in
28 paragraph (1) among an entruster or entrusters and a data trustee under which the data trustee is
29 empowered and directed to make decisions about use and onward supply of the data in furtherance

1 of the stated purpose. Despite this generality, and the wide-open possibilities that it suggests, some
2 types of data trust contracts that are found at present can be identified and described.

3 For example, one common type of data trust contract (as that term is used in this Principle)
4 is a data management contract, under which one party undertakes to manage data on behalf of
5 another party. An example is provided by personal information management services (PIMS), also
6 sometimes known as personal data stores, personal data spaces, or personal data vaults, under
7 which the party undertaking to manage the data (the ‘data trustee’ under the nomenclature of this
8 Principle) is empowered to make decisions on behalf of the entruster with respect to intellectual
9 property issues, data protection, etc. Such arrangements involve a requirement that the data trustee
10 manage the data for the interest of the entrusters and follow directions that they may give, subject
11 to the entruster’s right to withdraw from the arrangement at any time. In some ways, such an
12 arrangement is akin to an agency arrangement, with the entruster as principal and the data trustee
13 as agent.

14 **Illustration:**

15 73. Individuals I_1 to I_n contract with a service provider M under an arrangement in which
16 I_1 to I_n provide to M access to certain personal information collected by and stored on
17 their respective mobile devices. M is given the power to interact with website operators
18 that seek personal information from visitors to their websites and disclose only such
19 information under such conditions as meets criteria established in the contract. The
20 contract is a data trust contract.

21 Another common type of data trust arrangement is an arrangement under which one party
22 (the data trustee) undertakes to control data it has been entrusted with for a stated purpose, e.g. data
23 donation for health research. As with the data management contract, the greater expertise of the
24 data trustee is a motivating factor in entering into the arrangement.

25 **Illustration:**

26 74. A large number of health care providers H_1 to H_n contract with data trustee T to transfer
27 to the trustee access to data about cases of certain infectious diseases so that the trustee
28 can manage the data and make it available under specified terms to inform disease-
29 control programs in order to target interventions and improve health service coverage.
30 This contract is a data trust contract.

1 *c. Structure.* The arrangement created by a data trust contract can take many forms. In some
2 cases, the data trust contract may result in the formation of a common law trust (in jurisdictions
3 where that concept exists), but this is not necessary. Similarly, the data trust contract may result in
4 the creation of other arrangements that use trust nomenclature even though they are not common
5 law trusts, such as a ‘Massachusetts Business Trust’ or a Delaware Statutory Trust or Purpose
6 Trust, but this is not necessary either. Rather, the distinguishing feature of the data trust contract is
7 the agreement pursuant to which decisions about access to and use of data are to be made
8 collectively in furtherance of the stated purposes and for the benefit of the beneficiaries. The form
9 of such an agreement, and the decision making structure that results from it, is not constrained by
10 these Principles; of course, other law, such as competition law and data privacy/data protection
11 law, may apply and, in some cases, place limits.

12 *d. Distinguishing between the data trust contract and legal structures it may create.* It is
13 important to distinguish the data trust contract – the contract among the entrusters and the data
14 trustee under which the governing structure is created – from law governing the structure itself.
15 For example, if the agreement calls for the formation of a common law trust, with a trustee holding
16 the data for the benefit of beneficiaries to whom the trustee owes a fiduciary duty, the law
17 applicable to such common law trusts applies. Similarly, if the data trust contract calls for the
18 formation of a typical for-profit corporation or a public benefit corporation, the law governing such
19 corporations governs their internal affairs. It should be noted, however, that the law governing
20 structures that may be created by a data trust contract often provides for a substantial role for private
21 ordering by agreement among stakeholders. Examples include shareholder agreements with respect
22 to a corporation and the terms of the trust instrument in the case of a trust. The data trust contract
23 can be seen, therefore, not only as the agreement to create a particular structure but also as an
24 agreement among the stakeholders in the context of that structure.

25 Thus, while the default terms provided by this Principle do not impose fiduciary duties in
26 data trust arrangements, the form or structure selected by the parties to effectuate their data trust
27 arrangement may do so. In such cases, the fiduciary duties are those created by the law governing
28 the form or structure, and those duties augment the duties imposed by this Principle.

1 *e. Default terms.* The default terms for a data trust contract as described in this Principle are
2 necessarily general in light of the variety of situations in which such a contract may be utilized and
3 the variety of arrangements that the parties may devise.

4 First, subparagraph (a) provides a term relating to the power to make decisions with regard
5 to use and onward supply of the entrusted data. Under this term, the data trustee is, by default,
6 given the power to make all types of decisions with regard to the data, i.e. in the event of doubt the
7 power vested in the trustee is broader rather than narrower. However, that power is always subject
8 to terms (b) and (c), i.e. to the furtherance of the stated purpose of the data trust contract and the
9 benefit of the beneficiaries and the legitimate interests of the entrusters, as well as to any specific
10 directions given by the entrusters.

11 **Illustration:**

12 75. Assume that in a scenario such as the one in Illustration no. 74 the agreement between
13 the health care providers and trustee T does not specify clearly which kind of decisions
14 T may take with regard to the data, i.e. it is unclear whether T may pass the data on only
15 to public bodies or may also sell the data to private companies. Under Principle 13(3)(a)
16 the trustee may make such decisions, subject to Principle 13(3)(b) and (c).

17 Second, subparagraph (b) provides that the data's trustee's primary obligation is to act in
18 furtherance of the stated purposes of the data trust contract for the benefit of the beneficiaries. This
19 is a critical point inasmuch as it means that gaps or incompleteness in the data trust contract will
20 be filled with terms that are primarily guided by the purpose of the contract (which may differ from
21 the private interests of the parties).

22 Third, subparagraph (c) provides a default rule directing the data trustee to follow directions
23 given by the entrusters. This rule has an important limit, however; the trustee need not (or even
24 must not) follow directions where the trustee could reasonably be expected to realise that the
25 directions are incompatible with the stated purposes of the data trust. Thus, unless otherwise
26 agreed, the stated purposes of the trust serve as an outside limit on the power of entrusters to direct
27 the data trustee.

28 **Illustration:**

29 76. If T in Illustration no. 75, by selling the data to private companies, would be
30 jeopardizing the legitimate interests of the health care providers, e.g. by potentially

1 disclosing very sensitive data about the patients treated by those health care providers
2 and putting the health care providers at risk of being sued by their patients for breach
3 of confidentiality, the power vested in T does not include the power to sell the data to
4 the private companies as this would be incompatible with Principle 13(3)(b). The health
5 care providers could, in addition, give binding directions to T under Principle 13(3)(c)
6 to refrain from selling the data. However, they could not give directions to T to sell the
7 data if this is in violation of the stated purposes of the data trust contract (e.g. if that
8 stated or manifestly obvious purpose includes protection of patients' rights).

9 Fourth, subparagraph (d) provides a default rule that protects entrusters from data trustees
10 who might use their position to benefit themselves rather than the entrusters. This rule prohibits
11 the trustee from using the data to serve its own ends rather than the purposes of the entrusters; more
12 generally, this rule directs data trustees to avoid conflicts of interest with respect to the data and its
13 stewardship. This is so irrespective of whether the use of the data would also be in violation of the
14 default term under Principle 13(3)(b).

15 **Illustration:**

16 77. If T in Illustration no. 75 decided to form a research company and use the data it has
17 been entrusted with for that company's own research, T would be violating the default
18 term under Principle 13(3)(d).

19 Fifth, subparagraph (e) addresses the ability of the entrusters to terminate the powers of the
20 data trustee. The term proposed enables the entrusters to terminate the powers of the data trustee at
21 any time (much like termination without cause in the corporate context). This right, however, is
22 limited to the extent necessary to take into account legitimate interests of the beneficiaries of the
23 data trust.

24 Finally, subparagraph (f) states that, upon termination, the data trustee must return any
25 entrusted data the trustee has retained, or any data derived from such data, and, when reasonable,
26 take steps to prevent further use of the data by any onward recipients. This provision is similar to
27 that of Principle 12(2)(e) and if the data trustee may also be considered a processor under Principle
28 12 (which may or may not be the case), the obligation to erase might follow from both Principles.

1 **Illustration:**

2 78. If in Illustration no. 71, health care provider H_x, which is among the health care
3 providers entrusting T with their data, decides that it no longer wishes to participate in
4 the arrangement, it may, under Principle 13(3)(e), terminate the arrangement with T at
5 any time. This would mean T may no longer take any decisions with regard to H_x's data.
6 If H_x had transferred the data to storage space within T's control, T would have to erase
7 that data. If T has passed the data on to others, the question whether T must also take
8 steps to prevent further use of the data by those onward recipients depends on whether
9 that is reasonable. What counts as 'reasonable' depends on many factors, including
10 applicable law (such as data protection/data privacy law), any potential adverse effects
11 on the entrusters and the terms of the contractual arrangements T has entered into with
12 the onward recipients in fulfilment of its duties as data trustee.

13 *f. Incorporation of default terms into governing principles of structure of the data trust.* In
14 light of the fact that, as noted in comment *d*, a data trust contract often calls for the creation of a
15 structure, such as a corporation or common law trust, that has its own governance principles that
16 allow for the autonomy of the parties to shape their relationship, paragraph (3) also provides that
17 the default terms may be effectuated by being incorporated into the governing principles of an
18 entity created pursuant to the data trust contract rather than into the data trust contract itself.

19 *g. Analogies.* As noted in paragraph (4), this Principle suggests two approaches to
20 identifying analogies as the source of rules to govern data trust contracts. The first is to take into
21 account whether the purposes of the data trust contract are primarily for the benefit of the entrusters
22 or broader constituencies. Law has, for quite a long time, often taken different approaches to
23 arrangements that are primarily for private benefit and those whose primary purpose is to advance
24 public interests rather than solely the private interests of the parties. Thus, if the purpose of the data
25 trust contract is public benefit, appropriate analogies should be drawn. Second, the nature of any
26 organizational structure created by the data trust contract can supply analogies. For example, if the
27 data trust contract contemplates the creation of a corporation that will manage and exploit the data
28 on behalf of the entrusters, an analogy to shareholder agreements in corporations would be useful.

1 **REPORTERS' NOTES:**

2 **U.S.:**

3 In the U.S., a data trust contract would be governed by the general law of contracts (see
4 generally, Restatement (Second) of Contracts). As is the case with all contracts, courts may supply
5 contractual terms to address matters not addressed by the parties. See § 5, *cmt. b* (“Much contract
6 law consists of rules which may be varied by agreement of the parties. Such rules are sometimes
7 stated in terms of presumed intention, and they may be thought of as implied terms of an
8 agreement.”). Restatement § 204 further provides that “When the parties to a bargain sufficiently
9 defined to be a contract have not agreed with respect to a term which is essential to a determination
10 of their rights and duties, a term which is reasonable in the circumstances is supplied by the court.”
11 Thus, paragraph (2) of this Principle can be seen as an enumeration of reasonable terms to be
12 applied to the issues addressed in the absence of agreement of the parties.

13 As to common law trusts, see generally Restatement of the Law (Third), Trusts. In
14 particular, see § 2 of that Restatement for a definition of the term “trust” and § 5 for an enumeration
15 of relationships that do not constitute trusts.

16 As for the nature of Massachusetts Business Trusts, see, *e.g.*, Comment, The Nature of
17 Massachusetts Business Trusts, 27 Yale L.J. 677 (1918). With respect to statutory trusts, see, *e.g.*,
18 12 Del.C. § 3801 *et seq.* For a data trust arrangement as to which there are no beneficiaries that are
19 distinct from the entrusters, one possible entity is the so-called “purpose trust.” See, *e.g.*, S. Dak.
20 Stat. §§ 55-1-20 *et seq.* For a hybrid version with some beneficiaries, some states have created
21 “hybrid purpose trusts.” See, *e.g.*, S. Dak. Stat. §§ 55-1-22.

22 Illustrations 74 to 78 are based on DiSARM (Disease Surveillance and Risk Monitoring
23 project). See <https://www.disarm.io/>.

24 **Europe:**

25 *a. Data trust arrangements generally and b. Typical trust arrangements.* In Europe, the
26 term ‘data trust’ has been on everyone's lips for quite some time, and these arrangements are often
27 seen as a panacea for a range of different problems in the data economy. One form of data trusts
28 are personal information management systems (PIMS), which are also supported by the European
29 Commission in its data strategy for Europe (cf. COM(2020) 66 final, p. 10) the German Data Ethics
30 Commission (Opinion of the German Data Ethics Commission, 2019, p. 133 ff.) and the Data
31 Strategy of the German Federal Government (Datenstrategie der Bundesregierung, 2021, p. 33 ff).
32 While mere privacy management tools (PMT) support data subjects in managing their personal
33 data, PIMS support data subjects with exercising some of the data subject's rights under data
34 protection law, such as withdrawal of consent or porting requests. The concept of ‘data trusteeship’
35 (cf. Christiane Wendehorst, Of Elephants in the Room and Paper Tigers: How to Reconcile Data
36 Protection and the Data Economy, in Sebastian Lohsse, Rainer Schulze and Dirk Staudenmayer
37 (eds.), Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, p. 327, 346 et seq.)
38 is somewhat broader, as it includes not only sophisticated PIMS, vested with a mandate to exercise
39 data rights on behalf of the data subject according to standardised directions and preferences, but
40 also the management of IP rights, like copyright in user-generated content, or the management of
41 non-personal data.

42 With Chapter III of the Data Governance Act (DGA, COM(2020) 767 final) the
43 Commission published a first legislative proposal on ‘data sharing services’. The proposal covers
44 three types of services in its Article 9(1): (a) intermediation services between data holders and
45 potential data users, including making available the technical or other means to enable such

1 services; those services may include bilateral or multilateral exchanges of data or the creation of
2 platforms or databases enabling the exchange or joint exploitation of data, as well as the
3 establishment of a specific infrastructure for the interconnection of data holders and data users; (b)
4 intermediation services between data subjects that seek to make their personal data available and
5 potential data users, including making available the technical or other means to enable such
6 services, in the exercise of the rights provided in the GDPR; and (c) services of data cooperatives,
7 that is to say services supporting data subjects or one-person companies or MSMEs, who are
8 members of the cooperative or who confer the power to the cooperative to negotiate terms and
9 conditions for data processing before they consent, in making informed choices before consenting
10 to data processing, and allowing for mechanisms to exchange views on data processing purposes
11 and conditions that would best represent the interests of data subjects or legal persons.

12 The first of these three types of data sharing services would be qualified as a data
13 marketplace contract under Principle 15. However, the types addressed by Article 9(1)(b) and (c)
14 of the Proposal would be data trust contracts within the meaning of Principle 13. The DGA
15 Proposal is unclear as to whether a data subject can delegate or even assign the exercise of the data
16 subject's rights to a data sharing service provider. Arguably, this is possible only to a very limited
17 extent (Recital 24 DGA).

18 *d. Distinguishing between the data trust contract and legal structures it may create.* In
19 Europe, different models as to ownership structure can be envisaged, the choice between them
20 being determined by the need to ensure that the interests of the trustee are aligned with those of the
21 individuals it represents (see Aline Blankertz, *Designing Data Trust*, 2020, p. 24). The main options
22 discussed are the following: (a) a private for-profit company that is sufficiently independent from
23 any other business in the data economy, which may imply restrictions on who may own how many
24 shares; (b) a not-for-profit collecting society of the kind we find in the area of copyright law; (c) a
25 State authority.

26 The Data Governance Act (DGA, COM(2020) 767 final) avoids conflicts of interests by
27 setting out that these intermediaries have to separate their data sharing services from other services
28 (Recital 26 DGA). This means that the data sharing service should be provided through a legal
29 entity that is separate from the other activities of the provider (Article 11(1) DGA). In addition,
30 these intermediaries should bear fiduciary duties towards the individuals, to ensure that they act in
31 the best interest of the data holders (Recital 24 DGA).

32 *e. Default terms and g. Analogies.* According to the definition in Principle 13, data trust
33 contracts would often be qualified as a 'trust' or a 'mandate' in Europe. A trust is typically defined
34 as a 'legal relationship in which a trustee is obliged to administer or dispose of one or more assets
35 in accordance with the terms governing the relationship to benefit a beneficiary or advance public
36 benefit purposes' (see Article X. – 1:201 DCFR). A mandate is a contract under which 'a person,
37 the agent, is authorized and instructed (mandated) by another person, the principal: (a) to conclude
38 a contract between the principal and a third party or otherwise directly affect the legal position of
39 the principal in relation to a third party; (b) to conclude a contract with a third party, or do another
40 juridical act in relation to a third party, on behalf of the principal but in such a way that the agent
41 and not the principal is a party to the contract or other juridical act; or (c) to take steps which are
42 meant to lead to, or facilitate, the conclusion of a contract between the principal and a third party
43 or the doing of another juridical act which would affect the legal position of the principal in relation
44 to a third party' (Article IV.D. – 1:101 DCFR).

45 In Europe, trustees are typically entitled to do any act in performance of the obligation under
46 the trust (see Article X. – 5:201 DCFR; Article V(1) of the Principles of European Trust Law),
47 which is also set out in Principle 13(3)(a). However, the powers of the trustee are typically limited

1 by restrictions in the trust terms and to such acts which an owner might lawfully do or a person
2 might be authorised to do on behalf of another (Article X. – 5:201 DCFR).

3 A trustee is generally obligated to exercise any power for the benefit of the beneficiaries or
4 the advancement of public benefit purposes, in accordance with the law and the trust terms (Article
5 X. – 6:101 DCFR; Article 5(2) of the European Principles of Trust Law). This is also set out as a
6 default term for data trustees in Principle 13(3)(b); however, if the entrusters are not the
7 beneficiaries, the trustee may act in a manner that is not inconsistent with the legitimate interests
8 of the entrusters of which the data trustee has notice. Such an obligation can also be found in
9 mandate contracts under which the agent must act in accordance with the interests of the principal,
10 insofar as these have been communicated to the agent or the agent could reasonably be expected to
11 be aware of them (Article IV.D. – 3:102 DCFR).

12 The trust terms or the public benefit purpose typically serve as an outside limit of the trust,
13 as is stated in Principle 13(3)(c). Therefore, a trustee is in breach of his contractual duty if he
14 exercises powers that are not in accordance with the law and the trust terms (Article X. – 6:101
15 DCFR; Article 5(2) of the European Principles of Trust Law). The duty to follow the directions of
16 the entruster is similar to directions under mandate contracts. An agent must generally follow any
17 direction by the principal (Article IV.D. – 4:101(2) DCFR). However, where the direction is
18 inconsistent with the purpose of the mandate contract or may otherwise be detrimental to the
19 interest of the principal, the agent has to warn the principal (Article IV.D. – 4:101(2)(b) DCFR). If
20 the principal does not revoke the direction without undue delay after having been warned, the
21 mandate is changed to the direction (Article IV.D. – 4:201(1)(b) DCFR). The default rule is further
22 similar to the obligation in mandate contracts under which the agent must act in accordance with
23 the interests of the principal, insofar as these have been communicated to the agent or the agent
24 could reasonably be expected to be aware of them (Article IV.D. – 3:102 DCFR).

25 Principle 13(3)(d) ensures the neutrality of the data trust by prohibiting the use of the data
26 for the data trustee’s own purpose. This restriction can also be found in the Proposal for a Data
27 Governance Act (COM(2020) 767 final), which stipulates that the provider may not use the data
28 for which it provides services for other purposes than to put them at the disposal of data users
29 (Article 11(1) COM(2020) 767 final). The same holds true for metadata collected in the course of
30 the service, which may only be used for the development of that service (Article 11(2) COM(2020)
31 767 final). The provider shall also act in the data subjects’ best interest when facilitating the
32 exercise of their rights (Article 11(1) COM(2020) 767 final). A similar duty can also be found with
33 regard to trusts; the trustee is obligated not to make use of the fund, or information or an opportunity
34 obtained in the capacity of trustee, to obtain an enrichment unless this is authorized by the trust
35 terms (Article X. – 6:109 DCFR).

36 The right to terminate a data trust at any time (Principle 13(3)(e) is identical to the right to
37 terminate a mandate contract (Article IV.D. – 6:101 DCFR); revocation of the mandate of the agent
38 is also treated as termination of the mandate contract (Article IV.D. – 6:101 DCFR). However, the
39 right to terminate contracts can also be restricted as with trusts where the right to terminate is
40 generally available for a beneficiary of the trust to the extent that it is for the beneficiary’s exclusive
41 benefit (see Article X. – 9:104 DCFR), but an entruster that is not a beneficiary is only entitled to
42 terminate the trust to the same extent that he might have revoked a donation to the beneficiary if
43 the benefit had been conferred by way of donation (Article X. – 9:103 DCFR).

44 The last default rule (Principle 13(3)(f)) corresponds with Article 28(3)(g) GDPR, which
45 stipulates that the processor shall delete or return all the personal data to the controller after the end
46 of the provision of services relating to processing, and delete existing copies unless Union or
47 Member State law requires storage of the personal data. Furthermore, Article 16(3) DCSD

1 (Directive (EU) 2019/770) provides that, upon termination of the contract, the trader shall refrain
2 from further use of content provided by the consumer under the contract.

3 **Principle 14: Data escrow contracts**

4 **(1) A data escrow contract is a contract among one or more parties planning to use data**
5 **(the ‘contracting parties’) and a third party (the ‘escrowee’) under which the escrowee**
6 **undertakes to make sure the powers and abilities of some or all of the contracting parties**
7 **with respect to the data are restricted (the ‘restricted parties’) so as to avoid conflict**
8 **with legal requirements, such as those imposed by antitrust law or data privacy/data**
9 **protection law.**

10 **(2) A data escrow contract and the relationships it creates need not conform to any**
11 **particular organizational structure. This Principle applies, with appropriate**
12 **adjustments, to the governing principles of any entity created pursuant to a data escrow**
13 **contract.**

14 **(3) Subject to agreement of the parties and to other principles that take priority under**
15 **Principle 5, the law should provide that the following terms are included in a data escrow**
16 **contract or are incorporated into the governing principles of any entity created pursuant**
17 **to the data escrow contract:**

18 **(a) The escrowee has such powers with regard to the data as are necessary for the stated**
19 **purpose of the data escrow contract;**

20 **(b) The escrowee must act in furtherance of the stated purposes of the data escrow**
21 **contract even if such action is inconsistent with interests of the contracting parties**
22 **that are distinct from the stated purpose of the data escrow contract;**

23 **(c) The escrowee must not follow any direction given by a contracting party that is**
24 **incompatible with the stated or manifestly obvious purpose of the data escrow**
25 **contract;**

26 **(d) The escrowee must refrain from any use or onward supply of the entrusted data for**
27 **its own purposes and must avoid any conflict of interest; and**

1 **(e) If the data escrow contract is terminated, each party has an obligation during the**
2 **winding-up of the relationship not to take actions that undermine the stated**
3 **purposes of the data escrow contract.**

4 **(4) In determining which rules and principles to apply by way of analogy, as provided in**
5 **Principle 5, to data escrow contracts, consideration should be given in particular to**

6 **(a) The stated purpose of the data escrow contract and the nature of the data and of the**
7 **parties involved; and**

8 **(b) The organizational structure of the relationships created by the data escrow**
9 **contract.**

10 **Comments:** *a. Scope.* This Principle provides a general overview of the legal principles
11 recommended for data escrow contracts. It is stated at a high level of generality because, as with
12 the case of data trust contracts, both the subject of data escrow contracts and their nature can vary
13 widely and data escrow contracts are still an emerging concept. The main difference between a
14 data escrow contract under Principle 14 and a data trust contract under Principle 13 is that the
15 purpose of a data escrow contract is to limit the powers of some or all parties contracting with the
16 escrowee, whereas under a data trust contract the trustee must, at the end of the day, follow the
17 directions and defer to the powers of the entrusters. This difference entails several consequences,
18 resulting in a set of default terms that is distinct from that under Principle 13.

19 *b. Purposes of data escrow arrangements.* The essence of a data escrow contract is that the
20 restricted parties either divest themselves of (full) control of data they hold, transferring that control
21 to a third party (the escrowee), or take steps to ensure they will never get (full) control of particular
22 data. It might seem anomalous for a party to voluntarily surrender or renounce control. There are,
23 however, situations in which, for regulatory reasons or the like, it is important for a person with
24 rights or powers with respect to data to surrender or renounce control of that data. Antitrust
25 considerations (and related demands of competition law) are one example of such a situation;
26 another example is provided by data privacy and data protection law. In such cases, the parties can
27 avoid running afoul of important legal rules by renouncing control of data that they would
28 otherwise have.

1 **Illustration**

2 79. European company C would like to use a customer management system, run by U.S.
3 software company S. In order to comply with European data protection law, C must
4 ensure its customers' personal data are not transferred to the U.S. unless there are
5 sufficient guarantees in place that ensure U.S. authorities cannot access the data merely
6 upon a request made to S. In order to be able to make the deal, C and S therefore enter
7 into an agreement with trusted third party E, according to which customer data will be
8 transferred to S only in encrypted form, and it will be only with the help of keys held
9 by E that it will be possible to decrypt the customer data. The arrangement between S
10 and E is a data escrow contract.

11 *c. Structure.* The arrangement created by a data escrow contract can take many forms. In
12 some cases, especially in legal systems in which escrow arrangements are common and well-
13 understood, the arrangement may be created by an agreement that spells out the terms of the escrow
14 arrangement. In other cases, however, the data escrow contract may provide for the formation of
15 an entity of sorts to hold the escrowed data. It is important to distinguish the data escrow contract
16 – the contract among the contracting parties and the escrowee under which the governing structure
17 is created – from law governing the structure itself. For example, if the agreement calls for the
18 formation of a public benefit corporation, the law governing such corporations governs its internal
19 affairs. It should be noted, however, that the law governing structures that may be created by a data
20 escrow contract often provides for a substantial role for private ordering by agreement among
21 stakeholders. Examples include shareholder agreements with respect to a corporation and the terms
22 of the trust instrument in the case of a trust. The data escrow contract can be seen, therefore, not
23 only as the agreement to create a particular structure but also as an agreement among the
24 stakeholders in the context of that structure.

25 *d. Default terms.* The default terms for a data escrow contract as described in this Principle
26 are necessarily general in light of the variety of situations in which such a contract may be utilized
27 and the variety of arrangements that the parties may devise. Accordingly, paragraph (3) identifies
28 only a small number of default terms, which are applicable to all of these arrangements in case the
29 contract is silent, and leaves it to the parties to adapt the arrangement to their relevant data escrow
30 model in detail.

1 First, subparagraph (a) provides the key governing principle – the escrowee has whatever
2 powers are necessary for accomplishment of the stated purposes of the data escrow contract.

3 Second, subparagraph (b) provides that the escrowee’s primary obligation is to act in
4 furtherance of the stated or manifestly obvious purposes of the data escrow contract. This is a
5 critical point inasmuch as it means that gaps or incompleteness in the data trust contract will be
6 filled with terms that are primarily guided by the purpose of the contract (which may differ from
7 the private interests of the parties). Moreover, subparagraph (b) provides that the escrowee has this
8 obligation even if its actions would be inconsistent with interests of the contracting parties that are
9 distinct from the stated purpose of the data escrow contract.

10 It follows from this rule that subparagraph (c) provides that the escrowee must not follow
11 directions from contracting parties where the directions are inconsistent with the stated or
12 manifestly obvious purpose of the arrangement.

13 **Illustration**

14 80. S and E in Illustration no. 79 did not agree on the exact conditions under which S may,
15 as far as necessary for software maintenance, get access to particular sample datasets.
16 This gap is to be closed by reference to the purpose of the data escrow contract, which
17 is compliance with European data protection law. So E must take whatever steps are
18 needed to ensure that the requirements of European data protection law are fulfilled.
19 This is so even where S (or even both S and C) directs E to transfer particular datasets
20 to the U.S.

21 Fourth, subparagraph (d) provides a default rule that protects contracting parties from
22 escrowees who might use their position to benefit themselves rather than the position of the
23 contracting parties. This rule prohibits the escrowee from using the data to serve its own ends rather
24 than the purposes of the contracting parties.

25 Finally, subparagraph (e) provides that if the data escrow contract is terminated, the
26 winding-up of the relationship must not occur in a way that poses a threat to the stated purposes of
27 the data escrow contract. In some circumstances, particularly when the purpose of the data escrow
28 contract is to ensure that the restricted parties do not have (full) control of the data, this may mean
29 that a substitute escrowee should succeed to the interest of the original escrowee, or that some other
30 mechanism be created to ensure that the purpose of the arrangement is not undermined, rather than
31 having control revert to restricted parties.

1 enumeration of reasonable terms to be applied to the issues addressed in the absence of agreement
2 of the parties.

3 The term “escrow” is traditionally used in the United States to refer to situations in which
4 the asset held by the escrowee is money. See, e.g., *Howard v. Chicago Transit Authority*, 931
5 N.E.2d 292, 297 (Ill. App. 2010) (“In an escrow contract, a grantor and a third party execute a
6 written instrument under which the grantor gives funds to the third party to hold until a designated
7 time when those funds are delivered to a grantee.”) Thus, the usage here, where the subject of the
8 escrow is data, rather than money, is an adaptation of that standard usage. Similar adaptations have
9 occurred in a variety of contexts, such as software source code escrow.

10 Europe:

11 *a. Data escrow contracts generally and b. purposes of data escrow arrangements.* Data
12 escrow models are used in Europe to ensure legal compliance. One example is the storage of car
13 accident data of connected vehicles. Section 63a para 1 of the German Road Traffic Act requires
14 motor vehicles with a highly or fully automated driving function to store position and time
15 information determined by a satellite navigation system if there is a change in vehicle control
16 between the driver and the highly or fully automated system. The vehicle owner must arrange for
17 the transmission of the relevant data to third parties if this is necessary for the assertion, satisfaction
18 or defence of legal claims. However, if the data is controlled by the manufacturer, the latter might
19 seek to avoid possible claims against itself. To overcome this difficulty, the introduction of an
20 intermediary has been proposed. The relationship among this intermediary, the manufacturer and
21 the car owner would qualify as a data escrow contract, because it would limit the manufacturer’s
22 powers as to the data.

23 Another example is data protection in the case of onward transfer after the *Schrems II*
24 Judgement by the CJEU (Case C-311/18 ECLI:EU:C:2020:559 – *Schrems II*), where data escrow
25 contracts under Principle 14 could serve as such supplementary measures, which has also been
26 highlighted by the European Data Protection Board (EDPB) in its most recent Recommendation
27 01/2020 (EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure
28 compliance with the EU level of protection of personal data, 2020). The EDPB stated that strong
29 encryption before transmission could provide an effective supplementary measure, if the keys are
30 retained solely under the control of the exporters or other entities entrusted with this task (EDPB,
31 Recommendations 01/2020, p. 22 f.). Thus, data escrow contracts under Principle 14 could be a
32 key element to ensure an equivalent level of protection of the personal data in onward transfers
33 from the EU to the U.S.

34 The involvement of trusted third parties has also been intensively discussed regarding the
35 avoidance of any infringement of Article 101(1) TFEU, especially in data pooling contracts. Data
36 sharing between competitors always bear a potential of creating anticompetitive effects due to the
37 possible exclusion of non-participating competitors, including potential future competitors who
38 have not yet entered the market. This is the case where the data contains relevant strategic and
39 competitive information, such as costs and prices (Björn Lundqvist, *Competition and Data Pools*,
40 (2018) *Journal of European Consumer and Market Law* 4, p. 146, 150). Therefore, it has been
41 suggested that the data may have to be limited in scope, or aggregated and anonymized (Jacques
42 Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, ‘Competition policy for the digital
43 era’, 2019, p. 96), which could be achieved by the establishment of a data escrow under Principle
44 14 that only supplies data without any indications as to the companies it comes from.

45 *d. Default terms and f. Analogies.* In Europe, data escrow contracts would mostly be
46 qualified as a ‘trust’ which is defined as a ‘legal relationship in which a trustee is obliged to

1 administer or dispose of one or more assets in accordance with the terms governing the relationship
2 to benefit a beneficiary or advance public benefit purposes’ (see Article X. – 1:201 DCFR).
3 Therefore, reference can be made to the Reporters’ Notes in Principle 13.

4 **Principle 15: Data marketplace contracts**

5 **(1) A data marketplace contract is a contract between a party seeking to enter into a data**
6 **transaction (the ‘client’) and a data marketplace provider, under which the data**
7 **marketplace provider undertakes to enable or facilitate ‘matchmaking’ between the**
8 **client and other potential parties to data transactions and, in some cases, provide further**
9 **services facilitating the transaction.**

10 **(2) Subject to agreement of the parties and to other principles that take priority under**
11 **Principle 5, the law should provide that the following terms are included in a data**
12 **marketplace contract:**

13 **(a) Insofar as the data marketplace provider undertakes to facilitate or enable a**
14 **particular step with regard to a transaction, it must provide reasonable support to**
15 **the client in complying with any legal duties applicable to that step;**

16 **(b) The data marketplace provider must refrain from any use for its own purposes of**
17 **data, received from its client, that is the subject of the anticipated transaction; and**

18 **(c) Upon full performance or termination of the contract, the data marketplace**
19 **provider must erase any data in its control that is the subject of the anticipated**
20 **transaction and that it has received from its client, and any data derived from such**
21 **data.**

22 **(3) In determining which rules and principles to apply by way of analogy, as provided in**
23 **Principle 5, to data marketplace contracts, consideration should be given in particular**
24 **to:**

25 **(a) whether, and the degree to which, the data marketplace provider gains control of**
26 **the data concerned; and**

27 **(b) whether, and the extent to which, the payment or other performance owed to the**
28 **data marketplace provider depends on the whether the matchmaking results in a**
29 **data transaction.**

1 **Comment:** *a. Scope.* Data marketplaces play an important role in the data economy. They
2 can connect suppliers and recipients of data that, without the help of an intermediary, would not
3 normally be able to find each other and enter into a data transaction without undue burden or
4 expense. The most common transactions facilitated by such intermediaries are contracts for the
5 transfer of data within the meaning of Principle 7, followed by contracts for access to data within
6 the meaning of Principle 8. A ‘data marketplace provider’ is defined, for the purposes of these
7 Principles, as an intermediary who engages in ‘matchmaking’ (*i.e.*, acts as an intermediary
8 facilitating transactions between suppliers and recipients of data). Usually, data marketplaces
9 provide a range of further services to the parties, such as providing the infrastructure for
10 transferring the data and any payment, assisting the parties in complying with legal requirements,
11 providing reputational ranking services or services related to complaint handling. There exists a
12 broad variety of types and business models, such as ‘one-to-one’, ‘one-to-many’ and ‘many-to-
13 many’ marketplaces. This Principle can be applied to each of these models. Some marketplaces
14 actually have control of the data supplied, whereas others restrict themselves to the matchmaking
15 between supplier and recipient.

16 Where data is supplied via a data marketplace, there are usually three contractual
17 relationships involved: the relationship between the supplier and the recipient, the relationship
18 between the supplier and the marketplace, and the relationship between the marketplace and the
19 recipient. Both the relationship between the supplier and the marketplace and between the recipient
20 and the marketplace are marketplace contracts within the meaning of Principle 15.

21 **Illustration:**

22 82. Truck fleet operator T wants to minimize the amount of time lost to required rest breaks
23 and meal breaks taken by its drivers. Through geolocation devices on T’s trucks, T is
24 aware of where its trucks are at all times but does not always know the most efficient
25 routing for those trucks to make sure that they are near appropriate rest and food
26 locations at the best time for breaks. T enters into a contract with intermediary I under
27 which I agrees to find a party that can supply real-time data as to rest and food locations
28 and estimated travel time to them in light of current weather and traffic conditions so
29 that T can use this information to direct its trucks to the most efficient locations for rest
30 and meal breaks. The contract between T and I is a data marketplace contract.

1 *b. Default terms.* As with other data contracts, Principle 15 provides several default terms
2 for data marketplace contracts. Each of the four supplied default terms imposes a duty on the data
3 marketplace provider. Paragraph (2)(a) obligates the provider to assist the client in complying with
4 legal duties that apply to the transaction facilitated by the data marketplace provider.

5 Paragraph (2)(b) obligates the data marketplace provider to refrain from processing for its
6 own purposes any data that is the subject of a data transaction that it enables or facilitates.

7 Paragraph (2)(c) obligates a data marketplace provider who enters into a data marketplace
8 contract to erase any data in its control that is the subject of the anticipated transaction and that it
9 has received from its client, and any data derived from such data, upon full performance or
10 termination of the contract.

11 **Illustration:**

12 83. Accommodations information provider P runs a website on which users can search for
13 hotels available in a particular location on a particular date and compare
14 accommodations and prices. This service enables P to amass significant data concerning
15 the number of people who are considering travel to those locations on particular dates.
16 P believes that this information would be very valuable to car rental companies that
17 have dynamic pricing models so they can adjust their rates in those locations based on
18 anticipated demand. P does not, however, have the expertise necessary to identify the
19 appropriate officials of car rental companies to propose entering into data transactions
20 with them. Accordingly, P enters into a contract with data marketplace provider I
21 pursuant to which I performs matchmaking between P and car rental companies to
22 enable P to enter into data transactions with those companies. To enable I to perform its
23 matchmaking most effectively, P supplies some of its data to I. When the contract
24 between P and I has been fully performed by I or has otherwise been terminated, I must
25 erase the data supplied to it by P.

26 *c. Application of other law by analogy.* Contracts with a party that provides matchmaking
27 services are well-known in a number of contexts outside the scope of these Principles. For example,
28 parties wishing to sell real property often contract with matchmakers to find buyers for the real
29 property, and potential buyers will often similarly contract with matchmakers to find appropriate
30 real property within the buyer's budget. Similarly, companies seeking loans often contract with

1 matchmakers that can match them with lenders that make loans to other companies in similar
2 circumstances. To the extent that, in the applicable jurisdiction, default rules and principles have
3 been developed for application to such matchmaking contracts, those rules and principles are
4 appropriate to apply to data marketplace contracts by analogy. In some jurisdictions, those legal
5 rules and principles differ depending on whether compensation is owed to the matchmaker only if
6 the matchmaking services are successful and whether the matchmaker obtains control over the
7 subject matter of the match.

8 **Illustration:**

9 84. R runs a website containing reviews and rankings of various consumer products. R
10 harvests location data with respect to customers who access reviews and rankings. Data
11 as to the number of such customers seeking information about consumer products in a
12 particular location has value to retailers in that location. R enters into a data marketplace
13 contract with intermediary I pursuant to which I will be paid a fee for each successful
14 match between R and a retailer with respect to such data; the fee is an agreed fraction
15 of the amount charged by R to the retailer. Under the data marketplace contract, I
16 receives no compensation except for the fee for successful matches. In determining
17 what legal rules and principles to apply by analogy to the data marketplace contract,
18 reference should be made to rules and principles developed for other similar
19 matchmaking contracts and, in particular, to those in which the matchmaker’s
20 compensation is determined by the number and magnitude of successful matches.

21 **REPORTERS’ NOTES:**

22 **U.S.:**

23 In the U.S., a data marketplace contract would be governed by the general law of contracts
24 (see generally, Restatement (Second) of Contracts). As is the case with all contracts, courts may
25 supply contractual terms to address matters not addressed by the parties. See § 5, cmt. b (“Much
26 contract law consists of rules which may be varied by agreement of the parties. Such rules are
27 sometimes stated in terms of presumed intention, and they may be thought of as implied terms of
28 an agreement.”). Restatement § 204 further provides that “When the parties to a bargain sufficiently
29 defined to be a contract have not agreed with respect to a term which is essential to a determination
30 of their rights and duties, a term which is reasonable in the circumstances is supplied by the court.”
31 Thus, paragraph (3) of this Principle can be seen as an enumeration of reasonable terms to be
32 applied to the issues addressed in the absence of agreement of the parties.

33 An increasing number of data marketplaces are available online. See, e.g., the IOTA Data
34 Marketplace, which can be viewed at <https://data.iota.org/#/>. For a discussion of enhanced

1 matchmaking services, see, e.g., Marshall W. Van Alstyne and Michael Schrage, The Best
2 Platforms Are More than Matchmakers (Harvard Business Review Online 2016), which can be
3 viewed at <https://hbr.org/2016/08/the-best-platforms-are-more-than-matchmakers>.

4 **Europe:**

5 *a. Data marketplace contracts.* The regulation of online platforms is one of the milestones
6 the European Commission has announced in its Digital Single Market Strategy (COM(2015) 192
7 final, p. 11 ff). A first major step was the adoption of the Platform to Business Regulation (P2B
8 Regulation, Regulation (EU) 2019/1150), which mainly contains transparency obligations. Most
9 recently, the European Commission proposed a Data Governance Act (COM(2020) 767 final),
10 which would also establish notification requirements and conditions for data sharing service
11 providers. Data sharing services covered by the Proposal include intermediation services between
12 data holders which are legal persons and potential data users, including making available the
13 technical or other means to enable such services; those services may include bilateral or multilateral
14 exchanges of data or the creation of platforms or databases enabling the exchange or joint
15 exploitation of data, as well as the establishment of a specific infrastructure for the interconnection
16 of data holders and data users (Article 9(1)(a) COM(2020) 767 final). This would fall under the
17 notion of a data marketplace within the meaning of Principle 15. Data marketplaces normally also
18 qualify as an ‘online platform’ within the meaning of the recently published proposal for a Digital
19 Services Act (DSA, COM(2020) 825 final). The DSA mainly contains exemptions of liability and
20 due diligence obligations for all providers of intermediary services and the due diligence
21 obligations are – at least under the proposal – only to be enforced by public authorities.

22 *b. Default terms.* The obligation under Principle 15(2)(a), that the data marketplace provider
23 that facilitates certain steps of the transaction must provide reasonable support to the client in
24 complying with any legal duties would, under most European jurisdictions, be qualified as an
25 ancillary obligation to the contract. Specifically with regard to data, similar obligations can be
26 found in the GDPR (Regulation (EU) 2016/679), e.g. among the obligations owed by a processor
27 vis-à-vis the controller. According to Article 28(3) GDPR, the processor must, inter alia, assist the
28 controller by taking appropriate technical and organisational measures, insofar as this is possible,
29 to respond to requests by data subjects to exercise their rights and to enable compliance with legal
30 obligations, taking into account the nature of processing and the information available to the
31 processor. This idea also underlies Article 22(7) DSA. Due to the fact that many obligations in e-
32 commerce can only be fulfilled with the help of the intermediary, the proposal sets out that the
33 ‘online platform shall design and organise its online interface in a way that enables traders to
34 comply with their obligations regarding pre-contractual information and product safety information
35 under applicable Union law’.

36 Principle 15(2)(b), which obligates marketplace providers to refrain from any processing of
37 the data that is the subject of the marketplace contract for their own purposes has similarities to the
38 default rule laid down in Principles 12(2), 13(3), 14(3) and the proposed Data Governance Act
39 (COM(2020) 767 final). The latter sets out a duty for providers of data sharing services to act in
40 the data subjects’ best interest when facilitating the exercise of their rights and to not use the data
41 for other purposes than to put them at the disposal of the data users (Article 11(1) Data Governance
42 Act).

43 Restrictions on the continued use of data after termination of the contract (Principle
44 15(2)(c)) can also be found in Principle 12(2)(e). In European law, Article 28(2)(g) GDPR provides
45 that the processor must delete or return all personal data to the controller after the end of the
46 provision of services relating to processing. Furthermore, the controller has the duty to erase

1 personal data without undue delay when the personal data are no longer necessary in relation to the
2 purposes for which they were collected (Article 17(1)(a)). Where a trader supplies digital content
3 or services to a consumer, Article 16(3) DCSD (Directive (EU) 2019/770) stipulates that upon
4 termination of the contract, the trader shall refrain from further use of the content, which is data
5 provided or created by the consumer when using the digital content or service supplied by the
6 trader.

7 *c. Application of other law by analogy.* In Europe, data marketplace contracts under
8 Principle 15 would generally be qualified as service contracts (see Reporters' Notes to
9 Principle 12).

10

Part III: Data Rights

11

Chapter A: Rules and Principles Governing Data Rights

12

Principle 16: Data rights

13

(1) Data rights may include the right to

14

**(a) be provided access to data by means that may, in appropriate circumstances,
15 include porting the data;**

16

(b) require the controller to desist from data activities;

17

(c) require the controller to correct data; or

18

(d) receive an economic share in profits derived from the use of data.

19

**(2) The data rights set out in Part III are not exhaustive; rather, a legal system may conclude
20 that parties should have additional rights of this sort. Accordingly, no negative inference
21 should be drawn from the absence of those rights in Part III.**

22

**(3) The rights set out in Part III are without prejudice to rights other than data rights that
23 a person may have against a controller of data with regard to that data, such as rights
24 arising from breach of contract, unjust enrichment, conversion of property rights, or
25 tort law.**

26

27

28

Comment: *a. The concept of data rights.* The Principles in Part III deal with legally
protected interests that arise from the very nature of data as information recorded in a machine-
readable format suitable for automated processing, stored in any medium or as it is being

1 transmitted (Principle 3(1)(a)); they do not, however, address intellectual property rights that may
2 exist in certain data (Principle 1(2)). Data as recorded information is a non-rivalrous resource,
3 which may be used by many different parties for many different purposes at the same time, and to
4 the generation of which many parties may have contributed in many different ways. These
5 attributes are taken into account as the foundation of a set of Principles that recommend the
6 recognition of a new data-specific class of rights, which may be called ‘data rights’. Rights of this
7 nature are being recognized to an increasing extent in data-specific legislation and case law
8 worldwide, mostly taking the form of access rights. These data rights are not purely contractual, as
9 they may exist between parties without any contractual link and they do not reflect ownership
10 notions in the traditional sense because traditional notions of ownership do not work well with
11 resources of a non-rivalrous nature.

12 **Illustration:**

13 85. Small airline A operates airplanes manufactured and sold by P, the engines for which
14 were supplied by engine manufacturer E. Data concerning the performance of the
15 engines is transmitted directly from the connected engines to D, a data analytics
16 company developing predictive maintenance services and belonging to the same group
17 of companies as E. A would like to have access to the engine data in order to get a better
18 idea of whether maintenance could be dealt with in a more cost-efficient way. Part III
19 deals, *inter alia.*, with questions such as whether A has a data right as against D to be
20 given access to certain data concerning performance of the engines in airplanes run by
21 A. This right would not arise from contract as there is no contract between A and D,
22 and not even between A and E. Without a data right to access to the data of the sort
23 recommended by these Principles, in order to obtain access to the engine data A would
24 need to insist on a term, in its contract with P to obtain the airplanes, that would require
25 P to include in its contract with E a right of buyers such as A to access the data supplied
26 to D. Requiring A to negotiate for this cascade of contracts, sometimes referred to as
27 ‘going along the links of the chain’ would be unduly costly and time-consuming.
28 Besides, existing contracts that P has with E, and that E has with D, may not be readily
29 re-negotiated.

1 *b. Typical data rights.* As has been mentioned, the most important type of data right, and at
2 the same time the type of data right that is the most specific to the nature of data as a non-rivalrous
3 resource, is data access rights. Given the broad definition of ‘access’, which may mean anything
4 ranging from merely being able to read data to being able to engage in varying degrees of
5 processing the data on a medium in the controller’s sphere, to full portability of the data, access
6 rights may come in many different forms. It is, however, not feasible for these Principles to
7 differentiate between those many different shades of ‘access’. Rather, the Principles deal with
8 access rights in general, allowing for flexibility as concerns the modalities of access.

9 Another important data right may be the right to require that a party desist from particular
10 data activities, which can include a right to require desistance from any control or processing of
11 data, i.e. to require erasure of data. This, too, is a right that is specific to the nature of data, in this
12 case the nature of data as a resource the generation of which many different parties have contributed
13 to in many different roles, and the use of which in a way that is not usually seen in the tangible
14 world or with other more traditional assets.

15 A related data right is the right to require correction of incorrect or incomplete data. Last
16 but not least, these Principles consider an exceptional right to require an economic share in profits
17 derived from the use of data. This, again, is specific to the nature of data as a resource the generation
18 of which parties have contributed to who did not volunteer to contribute, and maybe were not even
19 aware they were contributing, and therefore did not have a fair chance to negotiate for
20 remuneration.

21 There may be other, related data rights not specifically listed in Principle 16(1), such as the
22 right to receive information about data held by a particular controller, which may be of a procedural
23 nature in some jurisdictions and a matter of substantive law in others.

24 *c. Difference between data rights under Chapters B and C.* Most of these rights, as set out
25 in Chapter B on rights in co-generated data, are justified by the share which a party had in the
26 generation of the data that is at stake: A party can have a share in the generation of data by providing
27 part of the content of the information coded in the data, e.g. the information is about something
28 that party has done or is likely to do, or by generating the code, e.g. that party drives a connected
29 car and that activity causes large amounts of information to be recorded, or by otherwise providing
30 a contribution to data generation within the meaning of Principle 18(1). Given that the share a party

1 had in the generation of data may justify very different data rights as listed in Principle 16(1), the
2 range of rights addressed in Chapter B is broad and diverse.

3 The data rights dealt with under Chapter B fulfil functions similar to those fulfilled by
4 ownership with regard to traditional rivalrous assets. However, the question of whether the bundle
5 of rights in co-generated data constitutes ‘property’ or ‘ownership’ is not addressed by these
6 Principles, as these Principles focus on the nature of the rights and not on their doctrinal
7 classification. Rights in co-generated data reflect a policy that whoever has contributed to the
8 generation of data should generally have some rights with respect to its use or with respect to the
9 value it generates. Unlike intellectual property rights, rights in co-generated data do not afford their
10 holder a clearly defined range of rights against everyone else to do something or to omit doing
11 something, but rather the data rights depend very much on the parties involved, and on the
12 particular situation.

13 As contrasted with the data rights addressed under Chapter B, which fulfill functions similar
14 to those fulfilled by ownership, those addressed in Chapter C are of a very different nature. They
15 are typically afforded to persons who did not have a share in the generation of the data but who
16 should nevertheless have a data right for other overriding considerations of a more public law
17 nature. Data rights within the meaning of Chapter C are, in reality, almost exclusively data access
18 rights, but might theoretically also include other forms of data rights.

19 *d. Non-exclusive character.* Part III sets out in some detail matters with respect to which
20 the law should provide for data rights. However, Part III is not intended as an exclusive list of such
21 rights. Rather, some states might decide that additional data rights should be recognized now, and
22 as the data economy develops and matures, states may well recognize further data rights and related
23 rights. Such related rights may facilitate the assertion of a data right in the first place, e.g., by giving
24 a right to be informed of whether the controller holds relevant data. Principle 16(2) clarifies that
25 the Principles do not exclude the existence of such additional data rights and related rights.

26 In a very similar vein, Principle 16(3) clarifies that Part III is without prejudice to any other
27 rights (i.e. rights that cannot genuinely be classified as ‘data rights’) following from existing bodies
28 of the law, such as arising from breach of contract, unjust enrichment, conversion of property
29 rights, or tort law, insofar as these rights might also arise in a data context.

1 **REPORTERS' NOTES**

2 **U.S.:**

3 As a general matter, it is almost axiomatic that U.S. law does not regulate the fairness of
4 arms'-length relationships as such. See, e.g., P.S. Atiyah, *Contract and Fair Exchange*, 35 U.
5 Toronto L.J. 1 (1985) (part of the traditional dogma of contract law is that "There is simply no
6 room for any inquiry into the fairness of the exchange"). There are quite a few exceptions to this
7 generalization, however. To mention just a few, transactions between corporations and their
8 directors are often subjected to a fairness test (see, e.g., Lawrence E. Mitchell, *Fairness and Trust*
9 *in Corporate Law*, 43 Duke L. J. 425 (1993), as are other matters between a fiduciary and
10 beneficiary.

11 In the context of transactions, the primary consideration of this sort comes from the doctrine
12 of unconscionability, which empowers judges to decline to enforce certain oppressive
13 arrangements. See UCC §§ 2-302 2A-108; Restatement (Second), *Contracts* § 208. While the
14 nature of what constitutes unconscionability is the subject of much controversy (see, e.g.,
15 Restatement of *Consumer Contracts* § 5), it is generally agreed that demonstrating
16 unconscionability requires more than showing that the arrangement is one-sided as a result of an
17 imbalance in bargaining power. See, e.g., UCC § 2-302 ("The principle is one of prevention of
18 oppression and unfair surprise and not of disturbance of allocation of risks because of superior
19 bargaining power." [internal citations omitted]).

20 Also, while there is general recognition that contracts of adhesion raise issues that do not
21 arise in fully-bargained contracts between those with comparable bargaining power, U.S.
22 jurisdictions differ as to the appropriate judicial response to that phenomenon.

23 Finally, the recognition that each party to a contract has a duty of good faith and commercial
24 reasonableness (see UCC § 1-304; Restatement (Second), *Contracts* § 205) constrains much
25 behavior that might otherwise seem to be allowable under a narrow reading of transactional
26 documents. See PEB Commentary No. 10 (1994) (explicating UCC concept of good faith
27 performance). See also Robert S. Summers, *Good Faith in General Contract Law and the Sales*
28 *Provisions of the Uniform Commercial Code*, 54 Va. L. Rev. 195 (1968).

29 **Europe:**

30 There are several examples in European law of what are referred to as data rights in these
31 Principles. However, the existing legal framework at the EU level is fragmented and consists of
32 several different instruments addressing specific data economy issues. Thus, existing data rights in
33 the EU are not guided by an overarching consideration or aim to address data economy issues on a
34 horizontal basis. In the *Data Strategy* (COM(2020) 66 final, pp. 13, 26 et seq.), the European
35 Commission proposed a more horizontal approach, clearly aligned with the concept of data rights
36 in relation to co-generated data set out in Part III, Chapter B of the Principles. In the proposed *Data*
37 *Act 2021*, the European Commission announced its intention to support data sharing between
38 companies, specifically addressing issues related to usage rights for co-generated data (e.g., IoT
39 data in an industrial setting), which are typically set forth in private contracts. The notion that data
40 rights will be a cornerstone in creating a robust legal framework for the data economy has gained
41 traction in academic literature worldwide. While various theoretical concepts are being developed
42 (see, e.g., Yuming Lian, *Data Rights Law 1.0*, 2019, pp. 105 ff, 155 ff), the principles aim to
43 provide concrete guidance on how to implement data rights.

44 Portability and access rights are closely related, but the exact delineation between the two
45 concepts is subject to scholarly debate (see Yannic Duller, *Facilitating Access to Data Silos*

1 (forthcoming); Sebastian Schwamberger, *Der Datenzugangsanspruch* (forthcoming)). However, it
2 is undisputed that the archetypes of portability law in Europe are Article 16(4) of the GDPR
3 (Directive (EU) 2019/770) for non-personal data and Article 20 of the GDPR (Regulation (EU)
4 2016/679) for personal data. Pursuant to Article 20 GDPR, data subjects have the right to receive
5 personal data concerning them, which they have provided to a controller on the basis of consent or
6 a contract, in a structured, commonly used and machine-readable format, and to freely transmit this
7 data to another controller. Where technically feasible, data subjects may request that the personal
8 data be transferred directly from one controller to another. The right to access data can also be
9 found in several sector-specific regulations. (See, e.g., Article 61 Payment Services Directive II
10 (Directive (EU) 2015/2366); Article 12 Electricity Directive (Directive (EU) 2019/944); Article 66
11 et seq. Type Approval Regulation (Regulation (EU) 2018/858); Article 27 REACH Regulation
12 (Regulation (EC) No. 1907/2006). While the former two access rights aim to avoid anti-
13 competitive lock-in effects to the detriment of customers and would thus be classified as Chapter
14 B rights (see Rapporteur's comments on Principle 20), the latter two rights would fall under Chapter
15 C as they are justified by public interest rather than co-determination considerations (see
16 Rapporteur's comments on Principle 24).

17 The right to require a controller to refrain from controlling or processing data appeared for
18 the first time in data protection law (see Article 12(b) and Article 14 of the predecessor Directive
19 95/46/EC of the GDPR). Pursuant to Article 17 of the GDPR, data subjects may request a controller
20 to erase data relating to them. In particular, the data subject has this right if the personal data are
21 no longer necessary for the purposes for which they were collected or otherwise processed, or if
22 consent to the processing has been withdrawn and there is no other legal basis for the processing.
23 Under the GDPR, data subjects may also request restriction of processing instead of erasure (see
24 Article 18). However, with the advent of the data economy, the right to obtain an injunction has
25 gained importance beyond data protection law and has also been incorporated into European
26 contract law. Due to the non-rivalry of data, the right to demand the cease and desist of data
27 processing fulfills a similar function as the right to reclaim physical goods. In the event of
28 termination of the contract for the provision of a digital service/content, Article 16(3) GDPR
29 requires the trader to refrain from using content other than personal data provided or created by the
30 consumer when using the digital content or digital service provided by the trader.

31 **Principle 17: Application of these Principles to data rights**

32 **Rights under Part III should be governed, in the following order of priority, by:**

- 33 (a) **rules of law that cannot be derogated from by agreement, including data**
34 **privacy/data protection law;**
- 35 (b) **agreement between the parties to the extent that the contract is consistent with**
36 **Principles 18 to 27 or there is freedom of the parties to derogate from Principles 18**
37 **to 27 under the applicable law;**
- 38 (c) **any applicable rules of the law other than those referred to in clause (a) that have**
39 **been developed for application to data rights; and**

1 **(d) Principles 18 to 27.**

2 **Comment:** Principle 17 fulfils, for data rights, a function similar to that fulfilled by
3 Principle 5 for data contracts. It sets out a general framework for the law governing data rights and
4 identifies the order of priority of the various possible sources of rules governing those rights.

5 As with Principle 5 for data contracts, mandatory rules of the applicable law take absolute
6 priority over rules from any other sources. Such mandatory rules may be rooted in concepts of
7 inalienable rights. They may, in particular, have their origin in data protection/data privacy law, or,
8 at least to a certain extent, in trade secrets law. Several regimes of protection of personal data (data
9 privacy) worldwide have introduced quite far-reaching access rights, porting rights, and rights to
10 request erasure or rectification of data, plus some other rights, such as restriction of processing.
11 These rights are vested in the data subject, i.e. the person to whom the personal data is referring.
12 Their logic is, notably in Europe, predominantly a fundamental human rights logic, but partly also
13 a property or competition law logic. Such rights, which cannot be derogated from by agreement,
14 are not affected by Principles 18 to 27, but Principles 18 to 27 may still be useful for their
15 interpretation and for gap-filling.

16 **Illustration:**

17 86. P frequently uses the services of platform operator O. When establishing an account on
18 the platform, P accepted O's data protection terms, including a term stating 'I agree that
19 O may use my personal data for personalising the content I see and the offers I receive,
20 and that for said purpose O will also pass my data on to third parties.' Later, when P
21 engages in online shopping, P receives offers exactly calculated to match P's estimated
22 maximum ability and willingness to pay, using, *inter alia*, data from P's personal diary
23 (which indicates, e.g., when P has commitment to be at distant locations and needs an
24 airplane ticket or the like to get there) with the result that P, on average, pays 30 percent
25 more than P would have paid if offers had not been personalised. At first sight, P may
26 be seen as having given consent, but Principle 21 may provide arguments for saying
27 consent should not be seen as valid (under doctrines of applicable law, such as doctrines
28 of unconscionability/unfairness), or that consent should be interpreted as not covering
29 the data utilization at hand.

1 Next, Principle 17 lists the agreement of the parties as a source of relevant rules and
2 principles. The conditions under which a person has a data right, and in particular the details of
3 such right, should ideally be defined in an agreement between the parties involved. However, an
4 agreement should govern only to the extent that it is consistent with Principles 18 to 27, considering
5 any need for interpretation or gap-filling, or to the extent that applicable law allows parties the
6 freedom to derogate from Principles 18 to 27 by agreement.

7 **Illustration:**

8 87. Assume that, in the situation described in Illustration no. 85, a contract between airline
9 A and engine manufacturer E explicitly excludes any kind of rights on the part of A to
10 access engine data. This contract would presumably – depending on the circumstances
11 of the individual case – be inconsistent with Principle 20. Whether or not it supplants
12 the rights provided in Principle 20 would depend on the extent to which Principle 20 is
13 subject to waiver. According to Principle 16(2) this depends on the (otherwise)
14 applicable law, i.e. it is only to the extent that the applicable law allows for such data
15 rights to be waived by way of contract that the contract would override Principle 20. In
16 any case, Principle 20 might be an argument for interpreting any contract clause on
17 waiver rather narrowly.

18 Next in order of priority come any rules of the law other than those referred to in clause (a),
19 i.e. other than mandatory, that have been (specifically) developed for data rights. As yet, there
20 seems to be no general (‘horizontal’) statutory regime of data rights, nor a regime created by case
21 law. However, this is in flux, and there is an increasing number of access rights and similar rights
22 in particular sectors, such as in the financial, energy and mobility sectors, and/or developed on the
23 basis of competition law.

24 Where there is neither any mandatory law, nor contractual provisions that override the
25 Principles, nor any specifically designed legal rules other than mandatory, Principle 17
26 recommends that rights should be governed by Principles 18 to 27. According to Principle 16(2)
27 this could occur within existing legal frameworks.

1 **REPORTERS' NOTES**

2 **U.S.:**

3 See generally Reporters' Notes to Principle 5, explaining the hierarchy of legal principles
4 applicable to contracts.

5 With respect to rules that cannot be derogated from by agreement, see Principles of the
6 Law: Data Privacy § 4. As stated in the Reporters' Note to that section, "American information
7 privacy law generally makes its notice requirements mandatory, and not subject to waiver by the
8 affected individual." See also California Consumer Privacy Act § 1798.192: "Any provision of a
9 contract or agreement of any kind that purports to waive or limit in any way a consumer's rights
10 under this title, including, but not limited to, any right to a remedy or means of enforcement, shall
11 be deemed contrary to public policy and shall be void and unenforceable."

12 For examples of remedies with respect to data rights, see, e.g., Principles of the Law: Data
13 Privacy § 14 and the extensive analysis of source material in the Reporters' Notes to that section.
14 See also, e.g., California Consumer Privacy Act § 1798.150.

15 **Europe:**

16 In Europe, the majority of specific statutory regimes on data rights are of a mandatory
17 nature. This applies to the rights in Article 16(4) DCS D (Directive (EU) 2019/770); Articles 61 ff
18 of the Type Approval Regulation (Regulation (EU) 2018/858), Article 12 Electricity Directive
19 (Electricity Directive (Directive (EU) 2019/944); Articles 66 f PSD II (Directive (EU) 2015/2366)
20 and Articles 15 ff GDPR (Regulation (EU) 2016/679).

21 However, statutory regimes of data rights also interact with contractual agreements. An
22 interesting illustration for this interplay is Title III (Articles 25 to 30) and Articles 118 and 119 of
23 the REACH Regulation (Regulation (EC) No 1907/2006). In order to strengthen the
24 competitiveness of the European industry, to avoid unnecessary testing (including on animals) and
25 to ensure that the Regulation is applied as efficiently as possible, provision is made for the sharing
26 of data between registrants on the basis of fair compensation. Where a substance has previously
27 been registered less than 12 years earlier the potential registrant shall, in the case of information
28 involving tests on vertebrate animals, and may in other cases, request from the previous registrants
29 certain information he requires. The potential and the previous registrant(s) shall make every effort
30 to reach an agreement on the sharing of the information requested. Such an agreement may be
31 replaced by submission of the matter to an arbitration board and acceptance of the arbitration order.
32 The previous and potential registrant(s) shall make every effort to ensure that the costs of sharing
33 the information are determined in a fair, transparent and non-discriminatory way. In order to allow
34 a potential registrant to proceed with the registration, even if an agreement with a previous
35 registrant cannot be reached, the European Chemicals Agency, on request, should allow use of any
36 summary or robust study summary of tests already submitted.

1 **Chapter B: Data Rights with Regard to Co-Generated Data**

2 **Principle 18: Co-generated data**

3 **(1) Factors to be taken into account in determining whether, and to what extent, data is to**
4 **be treated as co-generated by a party within the meaning of Principles 19 to 23 are, in**
5 **the following order of priority:**

6 **(a) the extent to which that party is the subject of the information coded in the data, or**
7 **is the owner or operator of an asset that is the subject of that information;**

8 **(b) the extent to which the data was produced by an activity of that party, or by use of**
9 **a product or service owned or operated by that party;**

10 **(c) the extent to which the data was collected or assembled by that party in a way that**
11 **creates something of a new quality; and**

12 **(d) the extent to which the data was generated by use of a computer program or other**
13 **relevant element of a product or service, which that party has produced or**
14 **developed.**

15 **(2) Factors to be considered when assessing the extent of a contribution include the type of**
16 **the contribution, the magnitude of the contribution (including by way of investment),**
17 **the proximity or remoteness of the contribution, the degree of specificity of the**
18 **contribution, and the contributions of other parties.**

19 **(3) Contributions of a party that are insignificant in the circumstances do not lead to data**
20 **being considered as co-generated by that party.**

21 **Comment:** *a. The concept of data rights in co-generated data.* Principles 18 to 23 reflect
22 the most important type of data rights, which are data rights based on the notion of co-generation
23 of data. A common denominator of these rights is that they find their justification in the share which
24 a party had in the generation of the data that is at stake: A party can have a share in the generation
25 of data by being the subject of the information coded in the data, or by being the owner or operator
26 of something that is the subject of the information, or by otherwise providing a contribution to data
27 generation within the meaning of paragraph (1). The reference to ‘operator’ in Principle 18 is to be

1 understood as referring to lessees or similar persons operating the relevant object in their own name
2 and on their own account. The share that the party had in the generation of the data is, however,
3 rarely the only justification. Rather, it is the share, together with the other factors listed in Principle
4 19(2) and further elaborated in Principles 20 to 23, that causes the data right in question to arise.
5 However, where a party does not have any kind of share in the generation of data, not even by
6 having invested in a data-generating device (which is the lowest-priority factor in the list provided
7 by paragraph (1)), a data right asserted by that party would not be based on Principles 18 to 23.

8 Whether only individual parties who have themselves contributed to the generation of data
9 (or their successors in interest, *e.g.* in a case of inheritance, merger or acquisition) can rely on
10 Principles 18 to 23, or whether also groups of persons, such as the citizens of a particular State, are
11 protected by these Principles is a difficult question, as is whether there are circumstances under
12 which one party can rely on a contribution made by another party.

13 **Illustration:**

14 88. Huge amounts of data generated by the citizens of a particular state is used by businesses
15 from another continent to develop sophisticated digital services and digital products,
16 which are then again sold to the citizens of the state of origin at a high price. Businesses
17 from the state of origin of the data do not have the practical ability to develop services
18 of their own because they do not have access to the necessary data. In scenarios as this
19 the question arises whether this state, or businesses resident in this state, can assert the
20 rights stated in Principle 20, arguing that ‘their’ population has generated the data.

21 While these Principles do not rule out that such collective data rights may exist, see
22 Principle 16(2), they do not address these rights.

23 *b. General factors.* Paragraph (1) is about the factors that determine what counts as co-
24 generation of data. The notion of ‘co-generation’ of data is a normative notion that does not
25 coincide with any notions of ‘generation’ of data that may be used in a more technical context. This
26 becomes visible in the first factor listed in paragraph (1) for determining whether data is co-
27 generated by a party – whether the party is the subject of the information coded in the data (*e.g.*
28 personal data, or data relating to a particular business and its activities), or is the owner or operator
29 of the subject of that information (*e.g.* data relating to the maintenance status of a machine, or to
30 the quality of a piece of land). While, from a technical point of view, such a person would not be

1 considered as having any share in the ‘generation’ of data unless that person has at the same time
2 contributed to recording the binary code or the like, the law may take a broader perspective. Being
3 the subject of the information may, from a legal point of view, even be the strongest form of
4 contribution, depending on the specific link between the information and the legitimate interest in
5 being provided access etc., or requiring desistance, or correction, or an economic share.

6 Another form of contribution of a party to the generation of data is that party pursuing an
7 activity by means of which data has been produced (e.g. that party has driven a connected car) or
8 owns or operates the device, by means of which data has been produced (e.g. the party owns the
9 machine that has generated the data). However, there are also other ways in which a party can
10 produce data by its activity, including by processing existing data in a way that potentially adds
11 value and makes it ‘new’ data. This is why Principle 18 must not be (mis)understood as applying
12 exclusively to the ‘first’ producer of data, but rather as applying to any producer.

13 Largely the same considerations apply to any party that does not produce data in the strict
14 sense of recording information that had not been recorded before but that assembles or structures
15 existing data in a way that creates something of a new quality, e.g. a database.

16 A party may have contributed to the generation of data also in other ways, such as by having
17 produced or developed a computer program or other relevant component of a product or service.

18 **Illustrations:**

19 89. User U is the owner of a connected car manufactured by P. Through the use of the
20 connected car by U, large amounts of data is generated, some of it related to the status
21 of the car itself (e.g. for purpose of predictive maintenance), some related to U’s driving
22 habits (e.g. for targeted advertising or dynamic insurance models), some related to the
23 environment (e.g. weather and traffic data). All of this data qualifies as having been
24 generated by both U and P, and possibly by other parties.

25 Paragraph (1) lists these factors and also states that the share which a party had in the
26 generation of data is to be assessed with a view to the degree of presence of these factors. Paragraph
27 (2) clarifies that the share a party has had in the generation of data depends on the type of
28 contribution (i.e. which and how many of the factors listed in Principle 18(1) are fulfilled), the
29 remoteness of the contribution (e.g., where an individual provides personal data to a controller the
30 share in the provided data is extremely high, but once the data has been pseudonymised or even
31 anonymised, the share becomes smaller and smaller), and the specificity of the contribution (e.g.,

1 where the same contribution could have been made by any other party, this has less weight than
2 when a contribution is specific for a particular party). Of course, the share also depends on the
3 contributions of other parties (e.g., the controller that has processed data in order to obtain derived
4 data, or that has inferred data from other data, may have a significant share in the generation of that
5 data, the extent of that share depending on similar factors as the ones just mentioned).

6 The factors partly reflect considerations of personality rights, partly they reflect the ‘labor
7 theory of property’ and partly they follow from the idea that the proceeds of property should
8 normally belong to the owner of the original property. The factors are listed in the order of their
9 relative weight. This does not mean an absolute order of priority, but a factor that figures lower in
10 the list normally needs to be present to a higher degree in order to have the same force as a factor
11 that figures higher. Very often, more than one factor is present in a particular case, e.g., where a
12 party generates data by driving their connected car, such data is at the same time identifiable to that
13 party and to a device owned by that party, in which case that party has co-generated the data both
14 under paragraph(1)(a) and paragraph(1)(b) and the contribution is potentially a particularly strong
15 one.

16 **Illustration:**

17 90. In Illustration no. 89 the share which U had in the generation of all three types of
18 data mentioned (status of the car, driving habits, environment) is quite high as it was by
19 U’s activity of driving the car, and by the data collecting functions of the car as a device
20 owned by U, that the data has been recorded. However, U’s share in generating the data on
21 personal driving habits is greatest, given the high degree of proximity and specificity and
22 the absence of comparably significant contributions from other parties. As compared with
23 U’s share in the other data types, the share in the generation of the weather and traffic data
24 is smallest. This is so because the data does not specifically relate to U or to U’s car, and
25 because manufacturer P’s contribution by designing the car’s sensors in a way that this data
26 is collected is significant in this case.

27 *c. Insignificant contributions.* Paragraph (3) clarifies that contributions of a party that are
28 insignificant in the circumstances do not lead to data being considered as co-generated by that
29 party. This is to avoid uncertainty and a situation where a controller of data is confronted with an
30 uncalculable number of parties asserting data rights based on a remote or minor contribution.

1 agreements and licenses)? What tools, mechanisms, or processes exist (or can be imagined) that
 2 may automatically enforce the rights, privileges, and controls of data ownership across distributed,
 3 complex information systems? Do existing, conflicting legal treatments of industrial data under
 4 copyright and database laws continue to work if clear ownership itself is defined now as an explicit
 5 starting point? How do certainty of ownership and the legitimate exercise of controls on the rights
 6 of ownership affect how data is economically valued as an asset of any company, business, or
 7 operating entity?" Frieden also notes that co-generation issues are particularly acute with respect
 8 to consumers. "Consumers are the primary subjects for the creation of data even though they may not
 9 actively participate. Consumers create useable data by filling in forms and disclosing personal
 10 information, but much more data gets created by their public, private and commercial activities. This
 11 means that consumers may not know whether and how data is being collected about a specific activity.
 12 Without voluntary or mandatory disclosure by the data collector, consumers may not even know the
 13 nature and scope of what information has been acquired, processed, analyzed and marketed.
 14 Accordingly, consumers have an interest in who collects, data, what they collect, when they do so, how
 15 they use the data and with whom they can sell or otherwise exchange the data."

16 **Europe:**

17 *a. The concept of data rights in co-generated data.* The idea of shared value creation of data
 18 has been recognized by the European Commission in its Communication 'Towards a common
 19 European data space' (COM(2018) 232 final, p. 10). This concept of non-exclusive rights in data
 20 competes with the idea, discussed for some time under the heading of 'data ownership', to
 21 introduce an exclusive data right (for details see Reporters' Notes to Principle 29). Meanwhile, the
 22 idea to introduce such an exclusive right has largely been dropped, and the concept of co-generated
 23 data has gained widespread recognition. The concept of 'co-generated data' developed by these
 24 Principles has already been adopted by the European Commission in its European Data *Strategy*
 25 (COM(2020) 66 final, p. 10), the German Data Ethics Commission (Opinion of the German Data
 26 Ethics Commission, 2019, p. 133 ff.) and the Global Partnership on AI, GPAI (see GPAI Working
 27 Group on Data Governance, A Framework Paper for GPAI's work on Data Governance, 2020).

28 *b. General factors and c. Insignificant contributions.* That a party's contribution to the
 29 generation of data is a very relevant factor for assigning data rights is particularly evident as far as
 30 personal data is concerned. Under the GDPR (Regulation (EU) 2016/679) data subjects have the
 31 right to access, port, rectify and erase data concerning them (see Reporters' Notes Principle 21 –
 32 23). While the GDPR's data rights are only granted to natural persons, some national data
 33 protection regimes also apply to legal persons (see Section 1 of the Austrian Data Protection Act
 34 (Datenschutzgesetz)). The current draft of the E-Privacy Regulation (ST_6087_2021_INIT) is also
 35 intended to apply to end-users irrespective of whether they are natural or legal persons
 36 (ST_6087_2021_INIT, Article 1(2)). Being the subject of information, however, is not only a
 37 relevant factor in data protection law. For example, where a bank customer wants to make use of a
 38 third party payment service provider, the customer may request from the bank to make all the
 39 relevant account and transaction data available to the payment provider (Article 66f PSD II,
 40 Directive (EU) 2015/2366).

41 In the data ownership debate, it was suggested that data be assigned to the person who
 42 actually triggers its generation, the so-called 'act of scripture' (see Thomas Hoeren,
 43 'Dateneigentum – Versuch einer Anwendung von §303a StGB im Zivilrecht', 2013 *MultiMedia*
 44 *und Recht*, p. 486, 487). The Principles partly reflect this notion by taking into account the extent
 45 to which data was produced by a party's activities. That a party, who owns and uses a product or
 46 service, has a legitimate interest in the data produced by that activity is – at least to some extent –

1 recognized by the DCSD (Directive (EU) 2019/770). If a contract for the supply of a digital
2 service/content is terminated, the trader shall refrain from using any content other than personal
3 data, which was provided or created by the consumer when using the digital content or digital
4 service supplied by the trader (16(3) DCSD, Directive (EU) 2019/770, see Reporters' Notes to
5 Principle 21). Furthermore, Article 16(4) DCSD entitles the consumer to have the content, which
6 was created during the use of the digital service or content, retrieved. Another example is Article
7 6(1)(h) of the recent proposal for a Digital Markets Act (COM(2020) 842 final), which obligates
8 gatekeepers to provide effective portability of data generated through the activity of business and
9 end users (see Reporters' Notes to Principle 20). The European Commission considered assigning
10 an exclusive 'data producer's right' to the owner or long-term user of a device (COM(2017) 9 final,
11 p. 13; Herbert Zech, 'Information as a tradable commodity', in: De Franceschi (ed.), *European
12 Contract Law and the Digital Single Market*, 2016, p. 51 ff.), but ultimately discarded the idea.

13 That a party processing existing data in a way that adds value should have rights in the
14 'new' data has similarities to the doctrines of production, combination and commingling of tangible
15 goods (for a comparative overview, see Brigitta Lurger and Wolfgang Faber, *Principles for
16 European Law - Study on a European Civil Code - Acquisition and Loss of Ownership in Goods*,
17 2013, p. 1150 ff., 1180 ff.). 'Production' is the process when a person, by contributing labour,
18 produces new goods out of material owned by that or another person. The producer becomes owner
19 of the new goods and the owner of the material is entitled, against the producer, to payment equal
20 to the value of the material at the moment of production, secured by a proprietary security interest
21 in the new goods (Article VIII.-5:201 DCFR; Article VIII.-5:201 PEL Acq. Own.). When goods
22 owned by different persons are commingled in the sense that it is impossible or economically
23 unreasonable to separate the resulting mass or mixture into its original constituents, but it is
24 possible and economically reasonable to separate the mass or mixture into proportionate quantities,
25 these persons become co-owners of the resulting mass or mixture, each for a share proportionate
26 to the value of the respective part at the moment of commingling (Article VIII.-5:202 DCFR:
27 Article VIII.-5:202 PEL Acq. Own.). The rules on combination under Article VIII.-5:203 DCFR
28 and Article VIII.-5:203 PEL Acq. Own. apply where goods owned by different persons are
29 combined in the sense that separation would be impossible or economically unreasonable. Where
30 one of the parts is to be regarded as the principal part, the owner of that part normally acquires sole
31 ownership of the whole, and the owner or owners of the subordinate parts are entitled, against the
32 sole owner, to payment secured by a proprietary security interest in the combined goods. Where
33 none of the parts is to be regarded as the principal part, the owners of the component parts become
34 co-owners of the whole, each for a share proportionate to the value of the respective part at the
35 moment of combination.

36 **Principle 19: General factors determining rights in co-generated data**

37 **(1) Data rights in co-generated data arise from considerations of fairness; accordingly, the**
38 **way they are incorporated in existing legal frameworks under applicable law and the**
39 **extent to which they may be waived or varied by agreement should be determined by**
40 **the role such considerations of fairness play in the relevant legal system.**

1 **(2) In the case of co-generated data, a party who had a role in the generation of the data has**
2 **a data right when it is appropriate under the facts and circumstances, which is**
3 **determined by consideration of the following factors:**

4 **(a) the share which that party had in the generation of the relevant data, considering**
5 **the factors listed in Principle 18;**

6 **(b) the weight of grounds such as those listed in Principles 20 to 23 which that party can**
7 **put forward for being afforded the data right;**

8 **(c) the weight of any legitimate interests the controller or a third party may have in**
9 **denying the data right;**

10 **(d) imbalance of bargaining power between the parties; and**

11 **(e) any public interest, including the interest to ensure fair and effective competition.**

12 **(3) The factors listed in paragraph (2) should also be taken into account for determining**
13 **the specifications or restrictions of data rights, such as concerning data formats, timing,**
14 **data security, further support required for exercise of the right to be fully effective, and**
15 **remuneration to be paid.**

16 **Comment:** *a. Relationship with existing legal frameworks.* Principle 19(1) describes the
17 rights under Chapter B as reflecting considerations of fairness. This means that their
18 implementation by courts or legislators should primarily occur within frameworks associated with
19 fairness, which differ from jurisdiction to jurisdiction. In many legal systems, and in particular for
20 cases where there is a contractual relationship between the parties, implementation will occur by
21 means of interpretation of the contract, applying doctrines such as unconscionability or principles
22 such as that of good faith and fair dealing, or via rules that control unfair contract terms, where
23 applicable. The Principles do not seek to indicate precisely how a jurisdiction should deal with the
24 matter, leaving the matter to domestic law. A legislator may also implement Part III of the
25 Principles as is, in which case a court might directly apply the Principles.

26 **Illustration:**

27 92. If a court is confronted with the question whether small airline A in Illustration no. 85
28 has a right against D to be provided access to the data, or a right against P that P arranges
29 contractual relationships with its suppliers in a way that allows A to access the data, the

1 court will do so within frameworks associated with fairness. As to the contract which
2 A has with P, the court may—depending on the applicable law—solve the issue by way
3 of contract interpretation according to good faith and fair dealing or resort to doctrines
4 such as that of contractual duties of care and consideration for the interests of the other
5 party, unconscionability, or B2B unfair terms control. If the applicable law considers the
6 relationship between A and M or D to be of a quasi-contractual nature that equally
7 comes with enhanced duties of consideration for the interests of the other party, a court
8 may use this tool. More generally, a court might, again depending on the applicable
9 law, resort to laws and doctrines on unfair commercial practices, abuse of dominant
10 market position, abuse of bargaining position, and the like.

11 Rights provided to a party under this Chapter may be waived or varied to the detriment of
12 that party by agreement to the extent that such waiver or variation is allowed under the legal
13 framework in which they are exercised. This means that the waivable or non-waivable nature
14 depends on the approach otherwise taken by the jurisdiction in which these Principles are
15 implemented, and that a jurisdiction may in turn differentiate (e.g., treat transactions with
16 consumers differently than business-to-business transactions). Accordingly, this Principle does not
17 propose a uniform concept of data rights. States that have a relatively strong tradition of private
18 ordering (at least in business-to-business transactions) may choose to have many or all of the
19 enumerated data rights treated as default rules, from which the parties may derogate by agreement.
20 Other states, however, may treat some or all of the data rights as mandatory rules or, perhaps, as
21 ‘sticky defaults’ from which derogation is not impossible but is accompanied by procedural or
22 substantive protections. For example, a jurisdiction that exercises strong control over unfair
23 contractual clauses even in business-to-business relationships may, in line with that general policy,
24 restrict waiver or variation of contract rules that might dilute that control. On the other hand,
25 jurisdictions that place greater reliance on the role of private ordering (at least in non-consumer
26 transactions) in the creation of efficient transactions are more likely to treat the rules in this Part as
27 default rules that are subject to contrary agreement of the parties. Even such jurisdictions, however,
28 may afford less flexibility for such private ordering in the context of transactions in a regulated
29 industry, such as the insurance industry.

1 *b. Determining factors.* The Principles identify five factors to be considered in determining
2 whether it is appropriate to afford to a party a data right. These factors are listed in Principle 19(2).
3 They are: (a) the share which the party seeking access had in the generation of the relevant data,
4 pursuant to the criteria set forth by Principle 18(1); (b) the weight of grounds such as listed in
5 Principles 20 to 23 which that party can put forward for being afforded the data right; (c) the weight
6 of any legitimate interests the controller or a third party may have in denying the data right,
7 considering Principles 20 to 23; (d) any imbalance of bargaining power between the parties; and
8 (e) any public interest, including the interest to ensure fair and effective competition. It is to be
9 noted that the competition aspect comes into play at various levels, and not only as a public interest:
10 in particular as far as the avoidance of lock-in effects is concerned, the ideal of fair and effective
11 competition may coincide with private interests. It is further to be noted that public interests may
12 both be an argument for and against granting access, so the fifth criterion works in both ways.

13 The factors listed in Principle 19(2) are not ordered by their relative weight, but should be
14 balanced against one another in a flexible manner. This means that if the ground a party brings
15 forward, e.g. under Principle 20, has particular weight, it may compensate for a relatively
16 insignificant contribution to data generation. Such flexibility is also necessary in order to enable
17 these Principles to be implemented by different legal frameworks, ranging from contract law, to
18 specific statutory regimes (horizontal or sectoral), to competition law, depending on the relevant
19 jurisdiction. Depending on the legal framework chosen by a jurisdiction to implement the
20 Principles it is even possible that a factor listed in Principle 19 is reduced to a degree of weight that
21 is almost negligible.

22 *c. Choice of factors.* As to the share a party had in the generation of the data, see Comments
23 to Principle 18. As to the weight of grounds which that party can put forward for being afforded
24 the data right see Comments to Principles 20 to 23. Legitimate interests in denying the data right
25 are, for instance, data protection or trade secret concerns.

26 Imbalance of bargaining power is a standard justification for legal systems to interfere with
27 private ordering for the protection of vulnerable groups, such as consumers, employees, tenants, or
28 authors with regard to their works. In competition/antitrust law, the idea appears both in the guise
29 of dominant market position in terms of a market share and, depending on the relevant jurisdiction,
30 of dominant position within a bilateral relationship. In some jurisdictions, there is an increasing
31 number of specific protective regimes for the benefit also of smaller businesses confronted with

1 bigger businesses, such as for SMEs marketing products or services via a platform. Where contract
2 law allows for the assessment of the fairness of an agreement, any imbalance in bargaining power
3 is an important argument that a court may take into account when assessing the deal. Principle
4 19(2)(d) may cover all of these scenarios, but is not intended to create any new form of ‘pseudo-
5 competition law’. Rather, jurisdictions will implement Principle 19 in a legal framework that fits
6 into the general legal landscape and does not cause any disruptive effects.

7 The relevance of the public interest within private relationships, in particular between
8 businesses, is normally very low, while it is the predominant idea underlying the data rights
9 addressed in Principles 24 to 27. However, public interests, such as the interest in ensuring fair and
10 undistorted competition, are always present to some extent, and where a State decides to implement
11 the Principles within its competition law, for instance, they may even already be seen as a
12 justification for data rights from very different point of views.

13 *d. Specifications.* A court or legislator grappling with co-generated data usually has at least
14 two decisions to make: Firstly, whether to grant a data right, and secondly, how this right must be
15 granted, i.e. what are the modalities with regard to formats, timing and the like, and whether access
16 must be provided for free or in return for appropriate remuneration. In taking the latter decision, a
17 court or legislator will have to consider, amongst other factors, the type and weight of the parties’
18 respective shares in the generation of the data (e.g. where a share consisted in considerable
19 monetary investment this may be an argument against giving the other party a free ride) and the
20 efforts required for complying with the right. In assessing what is appropriate in the circumstances,
21 the factors listed in paragraph (1) have to be taken into account.

22 **REPORTERS’ NOTES:**

23 **U.S.:**

24 See Reporters’ Note to Principle 18.

25 **Europe:**

26 *a. Relationship with existing legal frameworks.* As whether, and if so for which sectors or
27 scenarios, new data rights in co-generated data should be introduced, much is still in a flux. The
28 Data Act 2021 will probably include usage rights for co-generated data (such as IoT data in
29 industrial settings), typically laid down in private contracts (COM(2020) 66 final, p. 13). However,
30 it is still unclear how contract law can be developed further to create the right incentives and support
31 parties in reaching fair and efficient data access regimes. The proposals range from introducing
32 data access on a fair, reasonable and non-discriminatory (FRAND) basis to new rules on fairness

1 control of B2B-contracts adapted to the digital economy (see Dirk Staudenmayer, Towards a
2 European Private Law of the Digital Economy?, in André Janssen and Hans Schulte-Nölke (eds.),
3 Researches in European Private Law and Beyond, 2020, p. 65, 86 ff). However, the European
4 Commission is cautious when it comes to data rights on a FRAND basis, and only seeks to
5 introduce such compulsory data rights where specific circumstances so dictate, i.e. data access
6 rights should only be sector-specific and only introduced if a market failure in this sector is
7 identified/can be foreseen, which competition law cannot solve (COM(2020) 66 final, p. 13).

8 *b. Determining factors.* The factors listed in this principle are also considered relevant by
9 the German Data Protection Commission when deciding whether to grant a data right (see Opinion
10 of the German Data Ethics Commission, 2019, p. 85 f.). A similar set of factors that has been
11 proposed includes: (1) establishing a functioning and competitive market for the data economy (2)
12 promoting innovation (3) protecting consumer interests with a particular focus on protecting the
13 privacy of natural persons (4) promoting additional public interests (Josef Drexl, Legal Challenges
14 of the Changing Role of Personal and Non-Personal Data in the Data Economy, in Reiner Schulze
15 and Alberto De Franceschi (eds.), Digital Revolution – New Challenges for Law, 2019, p. 11 ff.;
16 id, Data Access and control in the area of connected devices, 2018, p. 51 ff.).

17 With regard to the significance of the share a party had in the generation of data see
18 Reporters' Notes to Principle 18. With regard to the grounds which a party relying on a data right
19 can put forward for being afforded that data right and the possible legitimate interests of the
20 controller or third party see Reporters' Notes to Principles 20 to 23.

21 A party's relative bargaining power is a standard criterion underlying much of the
22 mandatory rules or 'sticky' default rules enshrined in legal systems in Europe. This certainly holds
23 true for the whole of consumer law, the introduction of which is justified, to a major extent, by the
24 consumer's relative weakness in bargaining power. Similar considerations have led to the
25 introduction of protective mechanisms for employees or tenants of residential premises. More
26 recently, and also with regard to co-generated data, the P2B Regulation (Regulation (EU)
27 2019/1150) has introduced some minimum rights for SMEs whose bargaining position vis-à-vis a
28 platform provider is usually very weak. Moreover, the Directive on Unfair Trading Practices in the
29 Agricultural and Food Supply Chain (Directive (EU) 2019/633) prohibits practices that deviate
30 from good commercial conduct in the agricultural sector if the supplier has a lower annual turnover
31 than the buyer and thus aims to address significant imbalances in bargaining power. An imbalance
32 between the controller and the data subject also has to be considered when determining whether a
33 consent is freely given under the GDPR (see Recital 43 GDPR). Also EU competition law is, to a
34 large extent, based on the idea that unequal bargaining power, which may arise with regard to a
35 particular relationship (such as a supplier-customer relationship) or more generally because of a
36 dominant market position may justify corrective mechanisms, including access and similar rights.

37 Public interests are widely recognised as justification for data sharing obligations, beyond
38 co-generated data (see Reporters' Notes to Principle 24). For example, data sharing under the
39 Clinical Trial Regulation is justified by the protection of public health and the fostering of the
40 innovation capacity of European medical research (see Recital 67 of Regulation (EU) No
41 536/2014). Data sharing under the MIFIR Regulation serves the protection of the financial market
42 (cf. Recitals 14 et seq. of Regulation (EU) No 600/2014), and sharing of information under the
43 Road Safety Regulation serves the safety of road traffic (Commission Delegated Regulation (EU)
44 No 886/2013). The justification for data sharing under the INSPIRE Directive (cf. Recital 1 of
45 Directive 2007/2/EC) is environmental protection and mandatory data sharing under the REACH
46 Regulation (Regulation (EC) No 1907/2006) serves public interests of avoiding unnecessary
47 testing on vertebrate animals.

1 *d. Specifications.* The factors set out by Principle 19 not only provide guidance on whether
2 to create a data right but also on how to implement it. The specifications of existing data rights in
3 European law vary to a large extent, which may best be illustrated by comparing the various
4 access/portability rights (for a detailed analysis see Inge Graef, Martin Husovec and Jasper van den
5 Boom, ‘Spill-Overs in Data Governance: The Relationship Between the GDPR’s Right to Data
6 Portability and EU Sector-Specific Data Access Regimes’ [2020] *Journal of European Consumer*
7 *and Market Law* 3). For example, the GDPR’s data portability right may be exercised free of charge
8 unless the requests are ‘manifestly unfounded or excessive, in particular because of their repetitive
9 character’, the controller can charge a reasonable fee or refuse to act (Article 12(5) GDPR). Under
10 the DCSD (Directive (EU) 2019/770), the consumer may retrieve any content other than personal
11 data, which was provided or created by the consumer when using the digital content or digital
12 service free of charge. In comparison, the PSD II (Directive (EU) 2015/2366) does not require
13 banks to grant payment service providers access to account information free of charge but merely
14 stipulates that the bank shall not discriminate against any payment service providers (Article
15 66(4)(c)).

16 The rights under the DCSD and the GDPR have to be fulfilled within a reasonable time
17 (Article 16(4) DCSD) or without undue delay and in any event within one month of receipt of the
18 request, but this period can be extended to two months where necessary (Article 12(3) GDPR).
19 Fulfilment periods of up to two months would of course be incompatible with the requirements of
20 payment initiation services, which require real-time access in order to provide a timely transfer.
21 Thus, Article 66(4)(b) PSD II provides that the relevant data needs to be made available
22 immediately after the receipt of a payment order.

23 Regarding the format of the data, Article 20 GDPR sets out that the data subject has the
24 right to receive the data in ‘a structured, commonly used and machine-readable format’. Hence, the
25 appropriate format may depend on the specific sector (Article 29 Working Party, Guidelines on the
26 right to data portability (2017) WP 242 rev.01, 17). That the PSD II does not specify or delegate
27 the standardisation of APIs is seen as a major shortcoming of the instrument and its access right
28 (see European Commission, Retail Payments Strategy for the EU, COM(2020) 592 final).
29 Standardization efforts in the banking sector are pursued by industry led initiatives (see Berlin
30 Group, NextGenPSD2).

31 **Principle 20: Access or porting with regard to co-generated data**

32 **(1) Grounds that, subject to Principle 19, may give rise to a right to access or to port co-**
33 **generated data include circumstances in which the access or porting is**

34 **(a) necessary for normal use, maintenance or re-sale by the user of a product or service**
35 **consistent with its purpose and the controller is part of the supply network and can**
36 **reasonably be expected to have foreseen this necessity;**

37 **(b) necessary for quality monitoring or improvement by the supplier of a product or**
38 **service consistent with duties of that supplier and the controller is part of the supply**
39 **network and can reasonably be expected to have foreseen this necessity;**

- 1 (c) **necessary for establishing facts, such as for better understanding by a party of that**
2 **party’s own operations, including any proof of such operations that party needs to**
3 **give vis-à-vis a third party, where this is urgently needed by that party and the**
4 **access to or porting of the co-generated data cannot reasonably be expected to harm**
5 **the controller’s interests;**
- 6 (d) **necessary for the development of a new product or service by a party where such**
7 **development was, in the light of that party’s and the controller’s previous business**
8 **operations, the type of their respective contributions to the generation of the data,**
9 **and the nature of their relationship, to be seen primarily as a business opportunity**
10 **of that first party; or**
- 11 (e) **necessary for the avoidance of anti-competitive lock-in effects to the detriment of a**
12 **party, such as by preventing that party from rightfully switching suppliers of**
13 **products or services or attracting further customers.**
- 14 (2) **Consistent with Principle 19(3), a right under paragraph (1) should be afforded only**
15 **with appropriate restrictions such as disclosure to a trusted third party, disaggregation,**
16 **anonymisation or blurring of data, to the extent that affording the right without such**
17 **restrictions would be incompatible with the rights of others, or with public interests.**
- 18 (3) **The controller must comply with the duties under Principles 32 for the protection of**
19 **third parties, and restrictions under paragraph (2) must in any case enable the**
20 **controller to do so.**

21 **Comment:** *a. General observations on access rights.* In practice, access rights and related
22 rights are the most important data rights to be exercised vis-à-vis a controller in the data economy.
23 Access to data is of utmost importance for players to be able to understand better and to improve
24 their own business operations, to develop new products and services, to have a better choice
25 between different suppliers, and many other purposes. Simple access to the data is sometimes
26 insufficient for satisfying the legitimate interests of the party relying on the right, and transfer of
27 data to that party or a third party may be required as well. Principle 20 focusses on spelling out in
28 greater detail what is a legitimate ground on which the party seeking access may rely. Paragraph
29 (1) lists some typical situations in which a party has a legitimate interest in obtaining access to data
30 or in having it ported. This list is not meant to be exhaustive.

1 Principle 20 may be decisive for a legislator or court for affording to a particular party who
2 has contributed to the generation of data a right to have access to data or to port data, as well as for
3 parties when negotiating an agreement or for standardization agencies and similar bodies when
4 defining best practices. A court could make use of this Principle, for example, when applying the
5 unconscionability/unfairness test to contract clauses that are subject to such a test.

6 *b. User-generated data.* An issue that has been troubling parties in the data economy, courts
7 and legislators alike is the issue of a user's right to access user-generated data, i.e. data generated
8 by the user through the use of a product or service. The relationship between a user/customer and
9 a controller of user-generated data raises a wide range of complex legal issues. Often, the customer
10 is in the weaker position because it is in need of the commodity supplied, has already paid the full
11 purchase price to the supplier, and did not focus on the issue of data rights at the time of the
12 purchase. This is shown in the following illustration.

13 **Illustration:**

14 93. Farm corporation F buys from seller S a 'smart' tractor manufactured by manufacturer
15 T. The tractor's operating software is set up so that F will not be able to use the tractor
16 unless, when initialising it, F accepts and enters into end user agreements with T and
17 businesses U and V acting in cooperation with T. The end user agreements are about
18 licenses to use embedded software and software to be downloaded on a mobile
19 telephone, and about digital services to be provided to F, including weather forecasts,
20 soil analyses, targeted recommendations concerning the use of particular fertilisers and
21 insecticides, and predictive maintenance. If anything goes wrong with these licenses or
22 services, F is in a weak position, having paid the full purchase price to S who will, under
23 many legal systems, not be responsible for what T, U and V are doing, or be responsible
24 only during a very short period after delivery.

25 As it is mainly within the discretion of the supplier (or producer) to what extent data that is
26 absolutely necessary for the use of the commodity will be stored in external locations outside the
27 sphere of control of the customer, the customer becomes increasingly dependent on the continuing
28 goodwill of controllers. This is why customers should, in certain cases, at least have a right to
29 obtain access to their user-generated data. A typical situation where this is justified is where normal
30 use of the relevant commodity by the customer, including any necessary repair, requires access to

1 the data. In such a case, the customer should have the right to obtain access to the data, or to
2 designate a person to whom access is given. This ground overlaps to a certain extent with the
3 ground of avoidance of lock-in effects.

4 **Illustration:**

5 94. The tractor of farm corporation F in Illustration no. 93 has been damaged in an accident.
6 Manufacturer T's authorized repair shop states the tractor cannot be repaired and
7 recommends that F buy a new tractor. F would like to have a second opinion from an
8 independent repair shop, but the independent repair shop cannot evaluate whether the
9 tractor can be repaired without access to data about the tractor held by T. F should be
10 able to access the data or designate the independent repair shop as a party to be given
11 access.

12 Suppliers of connected commodities can also control the resale of the commodities even
13 where the law would normally not allow them to do so. Under the current law, control of
14 redistribution may be rightful, at least to a certain extent, in the realm of copyright protected works,
15 but usually not where ordinary tangible property is supplied in return for a purchase price. Where
16 the customer is allowed to resell, the controller of user-generated data should not be allowed to
17 discourage or prevent the customer from reselling by withholding user-generated data or in similar
18 ways. Rather, the customer may have a right against the controller to take all necessary steps in
19 order to put a third-party buyer in the same position as the customer. This follows from Principle
20 19(3) according to which access rights may have to be afforded with further support required for
21 exercise of the right to be fully effective.

22 **Illustration:**

23 95. Farm corporation F in Illustration no. 93 wants to resell the tractor to G. However, if
24 the transaction is to make sense in economic terms, resale of the tractor would require
25 that G be able to utilize all the data accumulated by F's use of the tractor. In order to do
26 so, G would also need further support, such as the ability to use software and digital
27 services that came with the tractor. F has a right to require T to take all necessary steps
28 in order to achieve this goal.

1 *c. Supplier-generated data.* With the Internet of Things, every step in a value chain
2 potentially generates data, and this data may be a valuable asset to more than just the party in the
3 value chain that happens to have collected and to control the data. A common situation where this
4 is the case and there is a particularly strong ground for requiring access to data is the situation
5 where a supplier, e.g. of components, needs access for the purpose of quality monitoring and
6 improvement consistent with its duties. This is particularly relevant where there is no direct
7 contractual link between the parties but where both parties are links in a supply chain or supply
8 network.

9 **Illustration:**

10 96. M is the company that produces the motors for the tractors produced by T. Data
11 concerning motor performance is collected, but not directly by T. Instead, V, one of the
12 cloud service providers cooperating with T, controls the motor data. M needs access to
13 the motor data in order to ensure the motors work as promised, in particular as M has
14 agreed to liability for losses that occur if motor problems exceed a particular threshold.
15 In this situation, M has a legitimate ground for obtaining access to the motor data.

16 *d. Establishing facts.* Frequently, the interest of the party seeking access to the data has
17 nothing to do with the value chain or value network in which that party and the controller are
18 involved. Rather, the party urgently needs access for establishing facts, such as for a better
19 understanding of its own business operations, or in litigation with a third party (to the extent this is
20 not already dealt with under procedural law in the relevant jurisdiction), and that access could not
21 possibly harm any interests of the controller. Again, this may constitute a legitimate ground.

22 **Illustration:**

23 97. F has sold a piece of land to third party D, and now D is suing F for an alleged breach
24 of a warranty. F would need data controlled by T to be able to prove, in the litigation
25 between F and D, that the soil was of a particular quality when D took over the land
26 from F. In this scenario F has a significant share in the generation of the data, is urgently
27 in need of the data, and providing the relevant dataset to F cannot reasonably harm T's
28 legitimate interests provided the dataset is limited and does not imply disclosure of any
29 of T's trade secrets.

1 98. B runs a shopping rewards plan under which customers shopping with particular
2 retailers earn reward points. Customer data is collected by B and used for customer
3 profiling and targeted advertising. C, who has just paid in cash at the shop of retailer R
4 and had the reward points credited to his account, is accused of shoplifting and arrested
5 by the police. C can prove his innocence by demonstrating that the purchase was
6 registered on the reward account and that he must therefore have paid for the goods. In
7 this case, very strong factors would weigh in favour of an access right on the part of C,
8 C having generated the information, being the subject of the information, and being
9 urgently in need of the data.

10 *e. Development of smart products or services.* Much of the data economy relies on the
11 development of innovative smart products or services. There are often several parties that would,
12 in principle, be in a position and willing to develop such products and services, and they may be
13 competing with each other. Such competition is normally good for innovation. However,
14 sometimes a party uses its position and bargaining power to monopolize huge amounts of data,
15 fencing off other businesses that may be as well-equipped, or even much better equipped, to exploit
16 the data's economic potential. Normally, the parties will enter into negotiations and transactions
17 and make a deal that leads to efficient outcomes, but sometimes this is not the case, e.g. because
18 one party abuses its dominant bargaining position.

19 **Illustration:**

20 99. M in Illustration no. 96 is the company that produces the motors for the tractors
21 produced by T. Data concerning motor performance on the road is stored by V, a
22 provider of cloud navigation services that cooperates with T. M would like to develop
23 a predictive maintenance service and would need access to the motor performance data
24 for this purpose. However, V refuses to give M access because V and T together plan
25 to start their own motor predictive maintenance service as a new field of business. In
26 this situation, consideration must be given to the fact that M is a motor company (and
27 V is not), that predictive maintenance is being developed with regard to motors
28 produced by M (and not by V), that M's contribution to the generation of the data is
29 very significant (while V's contribution is, in the first place, to just collect the data),
30 and that V is simply a service provider who should normally not be using such data for

1 its own purposes anyway. In the light of these circumstances, developing predictive
2 maintenance services for its own motors with the help of the data thus appears to be a
3 business opportunity primarily for M. M may, subject to the other factors mentioned in
4 Principle 19, thus have an access right against V. This access right of M is without
5 prejudice to the possibility that M may even have a right against V to require V to desist
6 from such data use.

7 *f. Prevention of lock-in effects.* User-generated data has huge potential to create ‘lock-in’
8 effects, e.g. the more user-generated data has been accumulated by a particular controller, the more
9 difficult it becomes for the user/customer to switch the supplier of a product or service. Suppliers
10 sometimes exploit this effect by strategic and often anti-competitive behavior, such as by raising
11 the price of commodities once the supplier has accumulated enough user-generated data for the
12 customer to be effectively ‘locked in’. From an economic perspective, this is an undesirable
13 situation, which is also likely to harm the customer’s legitimate interests. This is why Principle 20
14 may provide the customer a right of access to the user-generated data or the right to have it
15 transmitted to another party.

16 **Illustration:**

17 100. Farm corporation F in Illustration no. 93 wants to buy a new tractor. As tractors
18 manufactured by T have become very expensive F decides to buy a similar, but less
19 expensive, tractor manufactured by U. However, in order to take full advantage of the
20 functionalities of this kind of tractor, including a variety of analytical tools based on
21 data collected from the same parcel of land in the past, F would need access to data
22 about that parcel of land controlled by T. Unless F has a right against T to have this data
23 transferred to U there is a situation where F is ‘locked-in’ and may effectively be
24 prevented from switching manufacturers, which would be both harmful to F and to
25 farmers and competition at large. Therefore, F has a right to access to the data collected
26 by the tractor.

27 101. Small business S markets goods over the online marketplace run by platform provider
28 P. Over the years, S has accumulated a bulk of very positive evaluations by customers,
29 expressed as 4.8 out of 5 possible credit ‘stars’ and many enthusiastic feedback
30 messages. When S seeks to move to another online marketplace (run by Q), S requests

1 to have the reputational data transferred to Q. In determining whether S has rights
2 against P to have the reputational data transferred, a court should take into account, inter
3 alia, that S has worked hard over many years to produce the information coded in the
4 data, that S is in need of the data for a legitimate interest, and that denying portability
5 of reputational data has anti-competitive effects.

6 Similar considerations may apply where a supplier needs access to data in order to be able
7 to attract further customers apart from the controller, i.e. lock-in situations do not only occur with
8 regard to users.

9 *g. Restrictions.* Paragraph (2) clarifies that, consistent with Principle 19(3), restrictions on
10 rights to access or port co-generated data may have to be imposed in order to protect legitimate
11 interests on the part of the controller or third parties. This means that a data right vis-à-vis the
12 controller is afforded only with appropriate restrictions such as anonymization or disclosure to a
13 trusted third party.

14 **Illustration:**

15 102.M in Illustration no. 96 is the company that produces the motors for the tractors
16 produced by T and requests access to the motor data held by cloud service provider V.
17 However, some of the motor data is data relating to identifiable natural persons within
18 the EU and is, at least potentially, subject to EU data protection law. In this case, a court
19 will afford the access right subject to appropriate safeguards and make sure M bears the
20 costs.

21 This is particularly important as paragraph (3) clarifies that the controller must comply with
22 the obligations under Principle 32 with regard to the protection of third parties. There might
23 theoretically indeed be a clash between the fact that a controller faced is on the one hand with a
24 data access right and on the other hand with an obligation to exercise due diligence and take
25 reasonable and appropriate steps for the protection of third parties under Part IV, Chapter A. As a
26 first step, third parties' rights had already been taken into account when weighing different factors
27 and deciding whether or not to afford the access right, cf. Principle 19(2)(c). If the outcome of this
28 is that the access right should be afforded, the second step is to determine the exact conditions,
29 such as concerning data formats or remuneration and other modalities under Principle 19(3) and,

1 more specifically, concerning third party protection under Principle 20(2). In doing so, a result
2 must be achieved that avoids any clash or inconsistency between the controller’s obligation to grant
3 access and obligation to comply with the duties under Principle 32. This is to be achieved by way
4 of legal, technical and/or institutional safeguards.

5 **Illustration:**

6 103. In Illustration no. 102 there could be a contract between M and V that imposes strict
7 obligations on M for the protection of the data subjects, including that data access and
8 processing is only allowed for a limited number of purposes. V could then grant access
9 to M in a secure environment controlled by V or T, with V or T monitoring processing
10 activities by M in that environment and making sure no data leaves the environment
11 that might cause harm to the data subjects.

12 **REPORTERS’ NOTES:**

13 **U.S.:**

14 Data porting rights are addressed extensively in Principles of the Law: Data Privacy § 9,
15 particularly in the context of user-generated data. As stated in Comment a to that section, “Data
16 portability permits a data subject to control her or his personal information and can also further
17 consumer choice among enterprises. If a data subject is not able to leave a service or platform with
18 his or her personal data, he or she may be ‘locked in’ to it. The result can be highly negative for
19 the development of a “market” for privacy and security, in which entities compete to develop pro-
20 privacy terms of service and increase their security standards. Data portability also helps safeguard
21 personal information when a legacy provider goes out of business.”

22 Perhaps the broadest U.S. statute providing for data portability is the California Consumer
23 Privacy Act of 2018. Section 1798.100(d) of that Act provides that “A business that receives a
24 verifiable consumer request from a consumer to access personal information shall promptly take
25 steps to disclose and deliver, free of charge to the consumer, the personal information required by
26 this section. The information may be delivered by mail or electronically, and if provided
27 electronically, the information shall be in a portable and, to the extent technically feasible, readily
28 useable format that allows the consumer to transmit this information to another entity without
29 hindrance. A business may provide personal information to a consumer at any time, but shall not
30 be required to provide personal information to a consumer more than twice in a 12-month period.”

31 In addition, there are quite a few precedents for sector-specific data portability rights in the
32 U.S. These rights are addressed in some detail in the Reporters’ Notes to Principles of the Law:
33 Data Privacy § 9, which should be consulted in this regard. Examples provided there include
34 telephone number portability (see Communications Act of 1934, as amended, 47 U.S.C. §§
35 251(b)(2) and 153(37); 47 C.F.R. § 52.21(n)) and health information within the scope of HIPAA
36 (see 45 C.F.R. § 164.524). With respect to electronic medical records, see Health Information
37 Technology for Economic and Clinical Health Act [HITECH Act], 42 U.S.C.A. § 17935(e)(1)
38 (providing that “[I]n the case that a covered entity uses or maintains an electronic health record
39 with respect to protected health information of an individual . . . the individual shall have a right to

1 obtain from such covered entity a copy of such information in an electronic format and, if the
2 individual chooses, to direct the covered entity to transmit such copy directly to an entity or person
3 designated by the individual, provided that any such choice is clear, conspicuous, and specific.”).

4 **Europe:**

5 For personal data, the most prominent example of a portability right in Europe is Article 20
6 GDPR (Regulation (EU) 2016/679). Under said provision, data subjects have the right to receive
7 the personal data concerning him or her, which he or she has provided to a controller on the basis
8 of consent or of a contract, in a structured, commonly used and machine-readable format and have
9 the right to transmit those data to another controller without hindrance, and even to have the
10 personal data transmitted directly from one controller to another, where technically feasible. The
11 objective of data portability is to enhance the data subject’s control over their data (Recital 68
12 GDPR) and to prevent ‘lock-in’ by enabling the data subject to switch providers (Article 29 Data
13 Protection Working Party, Guidelines on the right to “data portability”, wp 242 rev.01, p. 5). Article
14 20 GDPR is based on considerations of facilitating the free flow of data rather than data protection,
15 which is underlined by the fact that exercising the right does not require the initial data holder to
16 erase the data.

17 If a consumer terminates a contract for the supply of digital content or a digital service due
18 to lack of conformity, the DCSD (Directive (EU) 2019/770) affords the consumer a data portability
19 right for non-personal data: According to Article 16 (4) DCSD, the consumer has, in the event of
20 termination, the right to request from the trader any content other than personal data, which was
21 provided or created by the consumer when using the digital content or digital service supplied by
22 the trader. The rationale of the rule is partly the rationale of restitution after the termination of a
23 contract, and partly reduction of lock-in effects as consumers might be discouraged to exercise
24 their right to terminate the contract if they would be deprived of access to the content they have
25 created by using the digital content or service (Recital 70 DCSD). However, the provision does not
26 create any additional obligation of the trader to retain data generated under a contract (cf. the initial
27 formulation in Recital 39 of the Commission Proposal (COM(2015) 634 final, which indicated
28 such an obligation).

29 Data access/portability rights can also be found in sectoral regimes. In the banking sector,
30 the PSD II (Directive (EU) 2015/2366) gives payers the right to allow third-party providers to
31 access their account information held by the payer’s bank in order to provide payment initiation or
32 account information services (Articles 66 f). This so-called ‘access-to-account’ rule is based on the
33 rationale that payers should be able to use innovative fintech services without being dependent on
34 the willingness of established banks to grant access to the data that is necessary to perform such
35 services. Since these third-party providers are likely to compete with established banks for a
36 lucrative line of business in the financial sector, the banks have an incentive to forestall competition
37 by denying access to the data required to offer the competing services, depriving payers of new
38 payment services. The payer, who co-generated the account data (see Principle 19), is the person
39 exercising the access/portability right and is also the primary beneficiary of the right. However, the
40 payment service providers are, of course, indirect beneficiaries of the access-to-account rule.

41 A data access right in the context of maintenance of assets is provided by Articles 61 ff
42 Type Approval Regulation (Regulation (EU) 2018/858), which requires vehicle manufacturers to
43 provide to independent operators unrestricted, standardised and non-discriminatory access to
44 vehicle on-board-diagnostics (OBD) information etc. However, there is a conceptual difference
45 between rights described above, in particular the PSD II, and the access right under the Type
46 Approval Regulation, as the latter is assigned to independent repair servicer proviers, who have not

1 contributed to the generation of the data. The car owners, who have a share in the generation of –
2 at least most of – the data are only the indirect beneficiaries of the rule. Hence, Article 66 ff of the
3 Type Approval Regulation would, under these Principles, rather qualify as a data right for the
4 public interest (see Chapter C); the public interest being a functioning aftermarket in the automobile
5 sector.

6 Most recently, data access and portability obligations, based on considerations of co-
7 generation, have been proposed in the envisaged Digital Markets Act (DMA, COM(2020) 842
8 final). In Article 6(h) the proposed Regulation obligates gatekeepers to provide business users or
9 end users effective portability of the data they provided or generated in the context of their use of
10 the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-
11 readable format. This should enable the business users and end users to port that data in real time
12 effectively and thus facilitate switching or multi-homing. In addition, Article 6(i) DMA obligates
13 the gatekeepers to grant business users, free of charge, effective, high-quality, continuous and real-
14 time access and use of data provided or generated by the business users while using the relevant
15 core platform services and also data inferred from the provided and generated data (see Recital 55
16 DMA). This also applies to data provided or generated by end users engaging with the products or
17 services provided by those business users.

18 Porting of data is also one of the essential elements of the Free Flow of Data Regulation
19 (Regulation (EU) 2018/1807). The Regulation applies to the porting of non-personal data in B2B
20 relationships and encourages the Commission to contribute to the development of EU-wide codes
21 of conduct to facilitate the porting of (non-personal) data in a structured, commonly used and
22 machine-readable format, including open standard formats (Article 6). On this basis, the SWIPO
23 (Switching cloud service providers and Porting of Data) Working Group, which is one of the
24 Digital Single Market Cloud Stakeholders Working Groups gathering more than 100 stakeholders,
25 adopted in November 2019 two draft Codes of Conduct. The first one is on Infrastructure as a
26 Service market and the second one on the Software as a Service market. These Codes of Conduct
27 will be assessed by the Commission by the end of 2022 (Article 8 of Regulation (EU) 2018/1807).

28 Article 9 of the P2B Regulation (Regulation (EU) 2019/1150) obliges the providers of
29 online platforms to disclose to business users the extent to which they will be granted access to
30 data (such as customer data). Initially the European Parliament's Committee on Transport and
31 Tourism proposed to grant commercial platform users a right to access all data collected by the
32 platform operators 'on the basis of the commercial activity of the respective business user'
33 (Amendment 58 of Opinion of the Committee on Transport and Tourism, COM(2018)0238 –
34 C8-0165/2018 – 2018/0112(COD)). However, the final provision is limited to a mere transparency
35 requirement. The ELI Model Rules on Online Platforms go one step further and call for a right to
36 port reputational data (Article 7: Portability of Reviews).

37 **Principle 21: Desistance from data activities with regard to co-generated data**

38 **Grounds that, subject to Principle 19, may give rise to a party's right to require that the**
39 **controller desist from data activities with regard to co-generated data, up to a right to**
40 **require erasure of data, should include situations in which**

1 **(a) the data activities cause, or can reasonably be expected to cause, significant harm,**
2 **including non-economic harm, to that party; and**

3 **(b) the purpose of the data activities is inconsistent with the way that party contributed**
4 **to the generation of the data, in particular because**

5 **(i) that party was induced to contribute to the generation of the data for an**
6 **entirely different purpose and could not reasonably have been expected to**
7 **contribute to the generation of the data if it had known or foreseen the**
8 **purpose of the data activities engaged in by the controller; or**

9 **(ii) that party’s assent to its contribution to the generation of the data for that**
10 **purpose was obtained in a manner that is incompatible with doctrines that**
11 **vindicate important public policies including those that protect parties from**
12 **overreaching conduct or agreements.**

13 **Comment:** *a. General observations on desistance.* While access rights within the meaning
14 of Principle 20 may be the most important type of data right, there are also cases where it may be
15 justified to afford to a party a right to require that the controller desist from a particular use of data
16 that party has co-generated. Whether it is appropriate under the facts and circumstances to provide
17 a party with such a right is determined by consideration of the factors listed in Principle 19.
18 Principle 21 explains in more detail what should count as a legitimate interest or ground for
19 requiring a controller of data to desist from using co-generated data (and, in some cases, to erase
20 it).

21 *b. Grounds to be put forward for desistance.* Grounds that may give rise to a party’s right
22 to require that the controller desist from using co-generated data include situations in which that
23 use is causing significant harm, including non-economic harm, to that party where the controller’s
24 purpose of use is inconsistent with the purpose for which that party was induced to contribute to
25 the generation of the data and that party could not reasonably have been expected to contribute to
26 the generation of the data if it had known or foreseen the purpose of use by the controller. In order
27 to make this judgment, and unless there are any indications that the individual party concerned had
28 different priorities and preferences, an objective test should be applied by default. The judgment

1 should be based on the assumption that there is effective competition and that the relevant party
2 had a choice.

3 **Illustrations:**

4 104. Manufacturer T of the smart tractor in Illustration no. 93 uses the data collected by the
5 tractor to create a database that can be sold to potential buyers of farmland, providing
6 extensive details about soil quality, in order to enable such potential buyers to make a
7 more informed decision regarding the price they would be willing to pay for the land.
8 The availability of this data would cause significant harm to F because such potential
9 buyers would have better information about the soil quality than F itself. F has
10 contributed to the generation of the data for an entirely different purpose (i.e. in order
11 to benefit from precision farming services), disclosing the data to buyers of land is
12 inconsistent with that purpose, and a person in F's position would not reasonably be
13 expected to produce the data if the person had known how T would make use of the
14 data. F has a legitimate ground to require that T desist from making the data available
15 to potential buyers.

16 105. Company X runs a social network. In contracting to use that social network, individual
17 Y expressly agrees, in the privacy statement, that X may use Y's photos and personal
18 contacts for any purpose X deems fit, including for profiling. X feeds all photos and
19 personal contacts into a database which is analyzed by artificial intelligence to create a
20 profile of Y. Employers are prepared to pay high prices for job candidates' profiles.
21 Because Y had uploaded several photos that show him drunk at parties, and this
22 information is revealed by his profile, potential employers who bought access to Y's
23 profile declined to offer Y a job on various occasions where, in the absence of the profile
24 information, the job would have been offered to Y. Y would not have agreed to the
25 contract with the social network had Y understood what might be implied by 'profiling'.
26 Y therefore has grounds to require that X desist from disseminating his profile.

27 There may also be cases where a party has given, or would have given, consent, e.g. due to
28 particular weaknesses or preferences, but obtaining that consent was incompatible with doctrines
29 that vindicate important public policies or those that protect parties from overreaching conduct or
30 agreements. Such public policies differ from jurisdiction to jurisdiction.

Illustration:

106. Assume that individual I in Illustration no. 105 was a young person with a very positive attitude towards anything digital and a ‘sharing is caring’ philosophy. Assume further that I was aware that any photos he might upload could become part of his profile accessible to some potential future employers, but took the position that he would not like to be working for people who do not ‘share his lifestyle’. Even if, ten years later, I is no longer comfortable that potential employers can have access to his profile that reveals embarrassing activities from I’s younger days, the test under Principle 21(1)(b)(i) would not be fulfilled. However, Principle 21(1)(b)(ii) might still apply if instigating a young person to risk their future career is held to be incompatible with public policy under applicable law.

REPORTERS’ NOTES:

U.S.:

See Principles of the Law: Data Privacy § 7(a): “Personal data shall not be used in secondary data activities unrelated to those stated in the notice required by Principle 4 without a data subject’s consent.” As stated in comment a to that section, “The concept of relevancy of personal data for the initial purpose and further processing means that data shall be tied to the initial use and not used for unrelated purposes.”

See also California Consumer Privacy Act § 1798.100(a) (“A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”)

As pointed out in the Reporters’ Notes for Principles of the Law: Data Privacy:

In 1973, the U.S. Department of Health, Education, and Welfare, in its influential report on the harms caused by computer databases, set forth a series of Fair Information Practices, one of which provides that “[t]here must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.” U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Commission on Automated Personal Data Systems 41-42 (1973).

In the United States, a number of federal statutes restrict secondary use. Among the key statutory provisions are the Privacy Act, 5 U.S.C. § 552a(e)(3)(B); Fair Credit Reporting Act, 15 U.S.C. § 1681b; Gramm–Leach–Bliley Act, 15 U.S.C. § 6802(c); Video Privacy Protection Act, 18 U.S.C. § 2710(e); Driver’s Privacy Protection Act, 18 U.S.C. § 2722(a); and Cable Communications Policy Act, 47 U.S.C. § 551(e).

These materials are analyzed extensively in those Reporters’ Notes, which should be consulted for additional details

1 **Europe:**

2 It is not easy to find direct equivalents of Principle 21. On the one hand, the most obvious
3 parallel would be the right to erasure ('right to be forgotten', cf CJEU in Case C-131/12
4 ECLI:EU:C:2014:317 – *Google Spain*) in Article 17 GDPR (Regulation (EU) 2016/679), whose
5 scope is limited to personal data. According to this right, the data subject has the right to demand
6 from the controller that personal data concerning him or her be deleted without undue delay if
7 certain conditions are met. This also includes the case that the personal data were originally
8 processed unlawfully, that the data subject has withdrawn his or her consent (if the processing was
9 based on this consent) or that the data subject has objected to the data processing (if he or she has
10 such a right to object). On the other hand, it should not be overlooked that the concept pursued by
11 Principle 21 (and by Part III as a whole) differs quite substantially from that of the GDPR. Not
12 only is Principle 21 also – or even primarily – written for non-personal data. Principle 21 also
13 departs from the approach adopted in the GDPR, according to which the consent to data processing,
14 once given, is the most important factor. This approach – like much else in the GDPR –not only
15 broader than European data protection law and impose disproportionate restrictions on the data
16 economy – especially for non-personal data, it is also not suitable to effectively protect those who
17 have contributed to the generation of data against those data activities that actually substantially
18 affect them. Indeed, once consent has been given and the formal requirements imposed by the
19 GDPR on the granting of consent have been met, it would seem that consent has also be given to
20 any self-harm or harm to others. In contrast, these Principles adopt a different approach, which
21 starts from the principle of free data processing, and only if a concrete data activity violates
22 fundamental principles of fairness, quite exceptionally a claim to defend oneself against such data
23 activities is provided.

24 Article 16 of the DCSD (Directive (EU) 2019/770) gives the consumer a right to require
25 desistance in case of termination of the contract for the supply of digital content or a digital service.
26 According to Article 16(3) the trader shall refrain from using any content other than personal data,
27 which was provided or created by the consumer when using the digital content or digital service
28 supplied by the trader. Article 16(3) also lists four cases where the interests of the trader outweigh
29 the interests of the consumer: the content (a) has no utility outside the context of the digital content
30 or digital service supplied by the trader; (b) only relates to the consumer's activity when using the
31 digital content or digital service supplied by the trader; (c) has been aggregated with other data by
32 the trader and cannot be disaggregated or only with disproportionate efforts; or (d) has been
33 generated jointly by the consumer and others, and other consumers are able to continue to make
34 use of the content. However, Article 16(3) DCSD also has a very different purpose than Principle
35 21 because Article 16 DCSD does not in any way refer to any harm suffered by the consumer.

36 The test in Principle 21(b)(i) faintly resembles the compatibility test set out in Article 6(4)
37 GDPR. Where a controller wishes to process data for a purpose other than that for which the
38 personal data have been collected the secondary purpose must be compatible with the primary
39 purpose, considering (a) any link between the purposes for which the personal data have been
40 collected and the purposes of the intended further processing; (b) the context in which the personal
41 data have been collected, in particular regarding the relationship between data subjects and the
42 controller; (c) the nature of the personal data; (d) the possible consequences of the intended further
43 processing for data subjects; and (e) the existence of appropriate safeguards, which may include
44 encryption or pseudonymisation.

45 An obligation to desist from the use of data that is based on considerations of unequal
46 bargaining power rather than data protection has been included in the recently proposed Digital
47 Markets Act (DMA, COM(2020) 842 final). Core platform services that function as gatekeepers

1 may have a dual role, i.e. provide core platform services to business users, while competing with
2 those same business users in providing services/products to end users. This dual role allows
3 gatekeepers to gain an advantage by using data, generated from transactions by their business users
4 on the core platform, for the purpose of their own services that offer similar services to that of their
5 business users. Thus Article 6(1)(a) DMA obliges gatekeepers to refrain from using any aggregated
6 or non-aggregated data, which may include anonymised and personal data that is not publicly
7 available, to offer similar services to those of their business users (see Recital 43 DMA).

8 **Principle 22: Correction of co-generated data**

9 **Grounds that, subject to Principle 19, may give rise to a party’s right to require that the**
10 **controller correct errors in co-generated data, including incompleteness of the data, should**
11 **include situations in which control or processing of the incorrect data may cause more than**
12 **insignificant harm, including non-economic harm, to that party’s or another party’s**
13 **legitimate interests, and the costs of correction are not disproportionate to the harm that**
14 **might otherwise result.**

15 **Comment:** Poor data quality is a major problem for the data economy. While normally the
16 controller itself should have the greatest interest in improving the quality of data controlled, there
17 may be situations in which the controller happens not to care, but another party who has co-
18 generated the data does care.

19 **Illustration:**

20 107. Business T produces tires that are supplied to car manufacturer C and installed on cars.
21 Data collected by the car sensors is supposed to reveal, inter alia, how well T’s tires
22 adapt to different weather conditions and road surfaces and how quickly the treads wear
23 off. Due to an error in programming the software in cars manufactured by C, the data
24 suggests that tires produced by T fail to adapt well to wet surfaces. This data is added
25 to a pool of car data, to which also other car manufacturers have access. While C may
26 not be sufficiently interested in correcting the data (e.g. because C itself is already aware
27 of the error and does not mind if its competitors draw inaccurate conclusions), T has a
28 strong interest in the error in the data being corrected.

29 It is in such circumstances that, according to Principle 22, a right should be afforded to the
30 other party to request correction of the data. Factors that should be taken into account are, once

1 more, all the factors listed in Principle 19(2). Among the legitimate interests the controller may
2 raise in denying the request are the costs and efforts of correction and the potential effectiveness
3 of such correction in preventing loss to the party seeking the correction. Given the general interest
4 to improve the quality of data in the data economy, rights to require correction will very often be
5 afforded, except when such a request is vexatious or totally unreasonable or otherwise abusive, or
6 disproportionately costly. If appropriate, in particular where the party requesting correction has
7 contributed to the incorrectness or incompleteness of the data, this party may have to bear a
8 proportionate part of the costs under Principle 19(3).

9 **REPORTERS' NOTES:**

10 **U.S.:**

11 Correction of data that is co-generated (within the meaning of that term in these Principles)
12 is addressed in Section 8 of the ALI's Principles of the Law: Data Privacy, which provides that "A
13 data controller shall provide a data subject with a reasonable process to challenge the accuracy of
14 the data subject's personal data" and that "When a data subject provides a reasonable basis in proof
15 to demonstrate that the data subject's personal data is incorrect, the data controller shall correct the
16 data by amending or deleting it, or by other means." Principles of the Law: Data Privacy § 8(d)(1)-
17 (2). As stated there, "One of the most universally accepted Fair Information Practice Principles
18 (FIPPs) concerns rights of access and correction." Principles of the Law: Data Privacy §8,
19 Reporters' Note 1. Federal law, both statutory and by administrative regulations, establishes some
20 rights of correction. For example, regulations under the Health Insurance Portability and
21 Accountability Act (HIPAA) provide that an individual has a right "to have a covered entity amend
22 protected health information," 45 C.F.R. § 164.526(a)(1). Also, the federal Privacy Act (which
23 addresses certain governmental records) provides that "[e]ach agency . . . shall (1) [permit an]
24 individual ... to review the record" and "(2) request amendment of a record." 5 U.S.C. § 552a(d)(2).

25 At the state level, the California Consumer Privacy Act does not provide for a right of
26 correction, nor would several other data privacy bills introduced in state legislatures. See, e.g.,
27 proposed Maryland Online Consumer Protection Act Maryland (S.B. 613, introduced February 4,
28 2019), proposed Massachusetts Consumer Data Privacy Act (S. 120, introduced January 11, 2019),
29 proposed Hawaii legislation "Relating to Privacy" (S.B. 418, introduced January 18, 2019), and
30 proposed North Dakota legislation relating to protection against the disclosure of personal
31 information (H.B. 1485, introduced January 14, 2019). In contrast, proposed New York legislation
32 provides that "on request from a consumer, the controller, without undue delay, shall correct
33 inaccurate personal data concerning the consumer." See proposed New York Privacy Act § 1103.2
34 (S. 5462, introduced May 9, 2019).

35 **Europe:**

36 A similar right can be found, in relation to personal data, in Article 16 GDPR (Regulation
37 (EU) 2016/679). The provision entitles the data subject to obtain from the controller, without undue
38 delay, the rectification of inaccurate personal data concerning him or her. The data subject also has
39 the right to have incomplete personal data completed, including by means of a supplementary
40 declaration. The provision applies in particular if the storage of such data violates the GDPR or

1 Union or Member State law to which the controller is subject (see recital 65 GDPR). Thus, the
2 provision aims to ensure one of the guiding principles of the GDPR, namely data accuracy, which
3 means that data must be accurate and, where necessary, kept up to date, and that all reasonable
4 steps must be taken to ensure that personal data which are inaccurate are erased or rectified without
5 undue delay (Article 5(1)(d) of the GDPR). In assessing whether inaccurate data must be erased or
6 rectified, the purpose for which the data are processed must be taken into account.

7 **Principle 23: Economic share in profits derived from co-generated data**

8 **(1) A party is normally not entitled to an economic share in profits derived by another party**
9 **from the use of co-generated data unless there is a contractual or statutory basis for**
10 **such a claim or it is part of an individual arrangement under Principle 19(3).**

11 **(2) Notwithstanding paragraph (1), in exceptional cases a party may be entitled to an**
12 **economic share in profits derived by a controller of co-generated data from use of the**
13 **data when**

14 **(a) that party's contribution to the generation of the data**

15 **(i) was sufficiently unique that it cannot, from an economic point of view, be**
16 **substituted by contributions of other parties; or**

17 **(ii) caused that party significant effort or expense; and**

18 **(b) profits derived by the controller are exceptionally high; and**

19 **(c) the party seeking an economic share was, when its contribution to the generation of**
20 **the data was made, not in a position to bargain effectively for remuneration.**

21 **Comment:** *a. General observations.* Whether producers of data should be entitled to an
22 economic share in the value created with the help of the data is a very controversial topic. Due to
23 the dynamic nature of data, the multitude of parties that contribute to the generation of data, and to
24 the nature of data as a non-rivalrous resource, it would be neither possible nor desirable to recognise
25 a general data right of that kind. Rather, where the situation is such as to allow a controller of data
26 to use the data rightfully and to benefit from the use that controller should be free to do so without
27 having to share the benefits with anyone else. To avoid injustice, however, paragraph (2) of this
28 Principle provides an exception under which a party can, in exceptional circumstances, obtain a
29 share of the profits.

1 The main reasons for not affording a general rule requiring remuneration for the use of co-
2 generated data are of a practical nature. Introducing claims for remuneration across the board, or
3 at least on a broad scale, would require encompassing and ubiquitous measurement of data flows
4 and make life for businesses and consumers alike much more complicated. It would be extremely
5 difficult to find a general remuneration scheme that is equitable, and given that businesses are likely
6 to pass the additional costs on to their customers in the form of higher prices for goods and services
7 it would, at the end of the day, result in customers who generate less data subsidising customers
8 who generate more data, which is questionable in itself from a policy point of view. In the light of
9 the fact that measurement of data flows, calculation of reimbursements and payment management
10 would itself mean additional costs, a general rule requiring remuneration might well mean less
11 prosperity for everyone. Further considerations include the creation of inappropriate incentives for
12 vulnerable individuals, such as minors or individuals in economic distress, to generate and disclose
13 as much data as possible.

14 *b. Monetary remuneration or compensation on other grounds.* Principle 23 addresses only
15 the possibility of a right to an economic share that is based exclusively on the fact that data has
16 been co-generated by the party exercising the right. It does not address rights to an economic share
17 based on other grounds, such as a contractual agreement. Likewise, where data is used wrongfully
18 there may be remedies on the part of any party whose rights have been harmed or infringed, and
19 such remedies may include the payment of money.

20 **Illustration:**

21 108. Driver D of a connected car produced by P contributes to the generation of large
22 amounts of data, including data collected by the car's sensors that are not related to the
23 functioning of the car or any services provided to D, which P then uses for creating very
24 valuable smart services. If, e.g., under applicable consumer legislation, the clause in the
25 contract between D and P about the use of D's car for this purpose is void, this may
26 give rise to a claim in unjust enrichment on the part of D.

27 Also, remuneration may be part of arrangements within the meaning of Principle 19(3).
28 However, independent and separate remuneration is normally not due.

1 *c. Exceptional nature of the right.* It is only under very exceptional circumstances that a
2 party may have an independent claim for an economic share in profits derived with the help of co-
3 generated data. Basically, this is the case under circumstances similar to those giving rise to
4 intellectual property rights and similar rights, i.e. there must either be a particularly unique
5 contribution or extraordinary investment. However, the threshold here is much higher than for
6 intellectual property rights, and there must be additional circumstances that make it unfair and
7 inconsistent with doctrines such as unjust enrichment for the party making the profit not to share it
8 with those who have contributed. Additional circumstances of this sort might arise from the
9 exceptional amount of profits derived by the controller, combined with the fact that, when the
10 contribution to the generation of the data was made, the contributing party was, for reasons
11 attributable (also) to the controller, not effectively in a position to bargain for remuneration.

12 **Illustration:**

13 109. Cancer patient P has an extremely rare genetic pattern, inherited from First Nation
14 ancestors, which allows him to overcome the cancer. Without telling P, hospital H uses
15 P's genetic data for developing a new method of cancer treatment, which H then sells
16 worldwide, deriving profits of several billion US dollars. This is a situation where the
17 data contributed by P is particularly unique, profits derived are exceptionally high, and
18 in the situation (P was being treated as a patient and worrying about cancer, P had no
19 idea about the value of the data) P was unable to effectively enter into negotiations with
20 H concerning remuneration.

21 However, if only the aggregate contributions of many parties contributing in the same way
22 or in similar ways to the generation of data have the effect described in Principle 23, those
23 contributors would not generally have a right to share in the profits.

24 **Illustration:**

25 110. Driver D of a connected car produced by M contributes to the generation of large
26 amounts of data, which M then uses, together with the data generated by thousands of
27 other drivers, for creating very valuable smart services, deriving profits of billions of
28 US dollars. Even if D's mobility profile may be unique, it can, from an economic point
29 of view, at any time be substituted with some other driver's data. Also, generating the

1 data does not require extraordinary effort or expense on the part of D. D does not have
2 a right to claim a share in M's profits.

3 REPORTERS' NOTES:

4 U.S.:

5 For a recent discussion of the issues raised here, see, e.g., Jorge L. Contreras, The False
6 Promise of Health Data Ownership, 94 N.Y.U. L. Rev 624 (2019).

7 Comment c and Illustration 82 are, of course, inspired by the story of Henrietta Lacks. See
8 Rebecca Skloot, *The Immortal Life of Henrietta Lacks*. It has been reported that "There are 17,000
9 U.S. patents that involve HeLa cells." "Can the 'immortal cells' of Henrietta Lacks sue for their
10 own rights?", *Washington Post*, June 25, 2018, viewed at
11 [https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-](https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/)
12 [henrietta-lacks-sue-for-their-own-rights/](https://www.washingtonpost.com/news/retropolis/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/), quoting Christina J. Bostick, an attorney who is
13 representing several descendants of Ms. Lacks. See also
14 <https://www.hopkinsmedicine.org/henrietalacks/frequently-asked-questions.html> (last visited
15 May 18, 2020), noting that "Johns Hopkins has never sold or profited from the discovery or
16 distribution of HeLa cells and does not own the rights to the HeLa cell line."

17 A well-known case rejecting an economic share of profits, albeit in response to a claim
18 raising somewhat different legal theories, is *Moore v. Regents of the Univ. of Cal.*, 793 P.2d 479
19 (Cal. 1990), cert. denied, 499 U.S. 936 (1991). But see *Greenberg v. Miami Children's Hospital*
20 *Research Institute, Inc.*, 264 F.Supp.2d 1064 (S.D. Fla. 2003) (finding that plaintiffs sufficiently
21 pled the requisite elements of an unjust enrichment claim).

22 Europe:

23 A major aspect of the discussion around 'data ownership' was the allocation of a fair share
24 of the economic value of data to parties who have contributed to the generation of data. Allocating
25 the income is normally a function of intellectual property rights (see Article 18 Copyright
26 Directive, Directive (EU) 2019/790). Suggestions were made, e.g., to have collective societies
27 manage individuals' economic rights in their personal data (cf. Karl-Heinz Fezer, *Repräsentatives*
28 *Dateneigentum – Ein zivilgesellschaftliches Bürgerrecht*, 2018, p. 84 f.). There has been strong
29 resistance against such a model, more or less for the reasons stated in the Comments to Principle 23
30 (e.g. Josef Drexl, *Data Access and Control in the Era of Connected Devices*, 2018, p. 144, Opinion
31 of the German Data Ethics Commission, 2019, p. 104 f.). There is, thus, currently no such right to
32 share in profits in Europe, and it seems unlikely that it will be introduced in the near future.

33 However, the factors listed as relevant for granting such a right in very exceptional
34 circumstances – uniqueness, investment, profit and lack of negotiability – are known from
35 European intellectual property law. Thus, the protection of copyright and similar rights applies
36 only if the work is the author's own intellectual creation (cf. Art. 1(3) Software Directive, Directive
37 2009/24/EC; Art. 3(1) Database Directive, Directive 96/9/EC), which requires that the work be
38 sufficiently original or unique (cf. CJEU Case C-5/08 ECLI:EU:C:2009:465 para. 37 – *Infopaq*).
39 The protection of investment made is provided by rights such as the *sui generis* right of the
40 Database Directive (see Article 7 of Directive 2009/24/EC). Finally, profit and the lack of
41 negotiability are the main arguments for protection until the first sale of a copy under the exhaustion
42 principle. The first sale of a copy of a computer program by the rightholder exhausts the distribution
43 right in that copy (cf. Article 4(2) of the Information Society Services Directive, Directive

1 2001/29/EC; Article 4(2) of the Software Directive), because the rightholder already had the
2 opportunity to obtain a fair remuneration at the first sale of the copy (cf. CJEU Case C-128/11
3 ECLI:EU:C:2012:407, para. 63 – *UsedSoft*). However, there are two important exceptions to this
4 principle: the first is that the author still has the right to control the subletting of the program or a
5 copy thereof (Article 4(2) of the Software Directive). The second exception is enshrined in Article
6 20 of the Copyright Directive (Directive (EU) 2019/790), which applies when the remuneration
7 originally agreed by the author turns out to be disproportionately low compared to any subsequent
8 relevant income from the exploitation of the works or performances. In such cases, the author - in
9 the absence of an applicable collective bargaining agreement - is entitled to demand additional,
10 reasonable and fair remuneration from the party with whom he has concluded a contract for the
11 exploitation of his rights.

12 Chapter C: Data Rights for the Public Interest

13 Principle 24: Justification for data rights and obligations

14 **(1) The law should afford data rights for the public interest, and for similar reasons**
15 **independent of the share that the party to whom the rights are afforded had in the**
16 **generation of the data, only if the encroachment on the controller’s or any third party’s**
17 **legitimate interests is necessary, suitable and proportionate to the public interest**
18 **pursued.**

19 **(2) Paragraph (1) is not intended to address intergovernmental relations.**

20 **(3) The proportionality test referred to in paragraph (1) should apply also for determining**
21 **the specifications or restrictions of data rights, such as concerning data formats, timing,**
22 **data security, further support required for exercise of the right to be fully effective, and**
23 **remuneration to be paid.**

24 **(4) If the law does not afford a data right but imposes a functionally equivalent data sharing**
25 **obligation, the Principles under this Chapter apply with appropriate adjustments.**

26 **Comment:** *a. Data rights motivated by the public interest.* Principle 24 refers to data rights
27 that are not based on the share that a party had in the generation of the data. A data right, in
28 particular a data access right, is conferred on a person that has no specific relationship with the way
29 the data was generated (i.e., the person is not the subject of the information and has not produced
30 or assembled the data). The type of data right addressed in Principles 24 to 27 is, therefore, of a

1 different nature from the rights addressed under Chapter B. While the rights provided in Chapter
2 B are clearly of a private law nature and follow something like a ‘property logic’, the rights
3 addressed in Chapter C are more of a public law nature. In practice, they are almost exclusively
4 about data sharing, i.e. data rights within the meaning of Principle 16(1)(a), but could theoretically
5 also include other types of data rights.

6 **Illustration:**

7 111. Farmer F has purchased a connected tractor, manufactured by M. After an engine
8 breakdown, F wants to have his tractor repaired at independent repair shop R. To repair
9 the tractor, R needs access both to data generated by the tractor while it was used by F
10 and to other data held by M to adjust the engine correctly. F himself would definitely
11 have a right under Chapter B to access the former data as it has been co-generated by F
12 (cf. Principle 20(1)(a)), and arguably also a right to access the latter data, taking into
13 account that this is further support required to make access to the co-generated data
14 fully effective (cf. Principle 19(3)). However, in order for independent repair shops like
15 R to fulfil their function properly it is not sufficient to give just F an individual right to
16 access data relating to F’s tractor—rather, R needs more general access to such data
17 held by M, e.g. in order to train and prepare for such types of repair. If the law affords
18 such access to R, this access is governed by the Principles under Chapter C, because R
19 did not share in the generation of the data.

20 Data rights within the meaning of Chapter C frequently overlap with competition law,
21 which primarily serves the purpose of ensuring undistorted competition for the benefit of everyone,
22 and may result in particular private parties having a data right against, for example, another party
23 with a dominant market position. There may be many other public interest considerations that can
24 lead a legislator to afford data rights of the sort addressed in this Chapter, such as enhancement of
25 research and development, more efficient use of research money and reduction of unnecessary
26 testing by imposing an obligation to share research data and results. There is also a growing debate
27 about the extent to which controllers of data can be forced to share certain data with actors in the
28 public services sector, such as in the health, mobility and energy sectors.

29 Given the variety of public interests potentially at stake, these Principles do not give specific
30 guidance as to the circumstances under which such data sharing obligations may be imposed.
31 Rather, these Principles restrict themselves to guidance concerning some core aspects which need

1 to be taken into account when a decision to impose such data sharing obligations or similar
2 obligations has been made. The notion of ‘public interest’ should be understood very broadly to
3 include rules that vindicate or establish private rights for reasons of the public interest. Antitrust
4 and competition laws are a good example of this phenomenon.

5 *b. Justification for encroachment.* The main purpose of Principle 24 is to clarify that the
6 affording of such data rights and the imposition of such data obligations amounts to an interference
7 with the interests of private parties and is thus in need of justification. In contrast, data rights and
8 data obligations under Chapter B may be seen simply as an attempt by the law to strike the right
9 balance between competing private interests. In deciding whether to afford data rights under
10 Principle 24, the public interest needs to be carefully weighed against the interests of the controller,
11 which may even be protected by fundamental rights. Data rights for the public interest may not
12 only encroach on the rights of the controller but also affect the protected interests of other parties,
13 such as data subjects (in the case of personal data) or the holders of IP rights (where the data is IP
14 protected). Their interests must also be duly taken into account when granting data rights for the
15 public interest. In the light of all these conflicting interests, the data right must be necessary and
16 suitable to achieve the objective and must be a proportionate means.

17 *c. Limited need for justification for open data in the public sector.* The considerations in
18 paragraph (1) relate primarily to governmental decisions to afford data rights against controllers in
19 the private sector. In the light of the complexities of intergovernmental relationships, paragraph (2)
20 provides that paragraph (1) does not address data rights as against a controller in the public sector.
21 A governmental decision to afford data rights against a data controller in the public sector raises
22 fewer issues than a decision to afford such rights against a data controller in the private sector
23 because, in the latter case, there is interference with economic rights of the controller while there
24 may not be such interference with economic rights in the case of public entities. It is often a purely
25 political consideration whether making public sector data freely available is a reasonable way of
26 helping the economy and spending the taxpayers’ money. Of course, if the controller is a public
27 entity and the data it controls are personal data or other data affecting legitimate interests of third
28 parties (such as those referred to in Principle 28), these third party interests still need to be fully
29 protected.

1 *d. Application of the proportionality test to modalities.* In line with Principle 19(3),
2 Principle 24(3) clarifies that the proportionality test applies not only to whether or not a right should
3 be afforded and/or an obligation imposed, but also to any specifications or restrictions, such as
4 concerning data formats, mode of access, timing, data security, further support required for exercise
5 of the right to be fully effective, and remuneration to be paid. In particular, remuneration of the
6 controller or other affected parties may be needed to make the imposition of an obligation a
7 proportionate measure.

8 **Illustration:**

9 112. Assume that the law grants independent repair shops, such as R in Illustration no. 111,
10 a data access right against the controllers of vehicle data such as M. In granting the
11 right, the law should make adequate provision for M's legitimate interests, such as
12 concerning protection of trade secrets, as well as the legitimate interests of third parties,
13 such as the trade secrets of any suppliers of components or, if the aggregated vehicle
14 data allows inferences with regard to other customers, the privacy and secrecy concerns
15 of other customers. This may mean that R should not be afforded a right to access all
16 tractor-related data on M's servers, but only to data that is necessary for R to fulfil its
17 functions, and data may need to be pre-processed so as not to allow inferences on other
18 customers or disclosure of trade secrets. Given also that R is acting for commercial
19 purposes it may be appropriate for the law to allow M to charge a reasonable fee.

20 *e. Functionally equivalent data sharing obligations.* Data rights afforded without regard to
21 a party's share in the generation of the data are mostly data rights afforded for the public interest.
22 Nothing in Principle 24 excludes the possibility that such data rights are afforded also with a view
23 to the protection or promotion of private interests, but it is much more common that private parties
24 are just the incidental beneficiaries of data rights, while the data rights were primarily afforded for
25 the public interest. This becomes all the more apparent in cases where the law primarily imposes
26 an obligation on the controller of data to share data with a particular class of parties, should these
27 parties be interested in the data, or even with the general public. Paragraph (4) therefore states that
28 the Principles under Chapter C apply with appropriate adjustments where the law does not focus
29 on the right, but instead on a functionally equivalent obligation.

1 requirements concerning access to the vehicle’s mechanical data. Under the proposed law,
2 dealers would have to provide prospective owners with, and prospective owners would
3 have to acknowledge receipt of, the notice before buying or leasing a vehicle. Failure to
4 comply with these notice requirements would subject motor vehicle dealers to sanctions by
5 the applicable licensing authority.

6
7 Massachusetts Secretary of State, "2020 Voter Guide."
8

9 The new law is the subject of a lawsuit by the “Alliance for Automotive Innovation” seeking
10 to enjoin enforcement on preemption and takings grounds. See United States District Court for the
11 District of Massachusetts, Case 1:20-cv-12090 Document 1 Filed 11/20/20. See also
12 [https://www.vice.com/en/article/93wy8v/newly-passed-right-to-repair-law-will-fundamentally-](https://www.vice.com/en/article/93wy8v/newly-passed-right-to-repair-law-will-fundamentally-change-tesla-repair)
13 [change-tesla-repair;](https://www.vice.com/en/article/93wy8v/newly-passed-right-to-repair-law-will-fundamentally-change-tesla-repair) [https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-](https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-not-users)
14 [not-users](https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-not-users)

15 **Europe:**

16 The European Union has already introduced several sector-specific instruments that grant
17 access rights to parties who have not contributed to the generation of the data. Since these access
18 rights need to be not only justified by a public interest but also necessary and proportionate, they
19 are limited to certain situations where the European legislator deemed the public interest to
20 outweigh the interest of the controller, and only cover data that is necessary to achieve the objective
21 pursued. Political consensus may develop for the adoption of additional data rights for the public
22 interest.

23 One of the most prominent examples for an access right against the controller by a party
24 that has not contributed to the generation of the data, is in the Type Approval Regulation
25 (Regulation (EU) 2018/858). Article 61 obligates car manufactures to grant independent
26 maintenance and repair service providers access to the technical information necessary to perform
27 their services in a non-discriminatory way for fees that are reasonable and proportionate. The
28 rationale of this access right is that, due to the complexity of today’s vehicles, independent repair
29 service providers, as well as spare part producers, can only offer their services and products if they
30 have access to the necessary technical information. Since the access right of the independent
31 service providers interferes with the contractual freedom of car manufacturers as well as their
32 freedom to conduct business (Article 16 Charter of Fundamental Rights), it needs to be justified by
33 a legitimate public interest. In this case, the public interest is to prevent a market failure on the
34 aftermarket, which would lead to higher prices, lower quality of services, less innovation, and less
35 choice for consumers. The market failure tendencies in the aftermarket in the automotive sector
36 have been a longstanding issue. Car manufactures try to forestall effective competition by denying
37 access to brand-specific technical information in order to promote authorized dealers and repairers,
38 which have proven to be very profitable for the manufacturers. However, by allowing the
39 manufacturers to charge a reasonable fee for the access, the Type Approval Regulation also takes
40 into account the legitimate interest of manufacturers to receive a fair return on their investment.
41 The Type Approval Regulation serves as an example for an instrument that primarily aims at
42 promoting a public interest (functioning aftermarket), although the access right is afforded only to
43 a handful of the private parties (independent repair and maintenance service providers), who thus
44 of course also benefit from the access right.

45 The public interest that justifies an access right may be something other than a functioning
46 market, as demonstrated by the REACH Regulation (Regulation (EC) No 1907/2006). Article 27

1 gives a manufacturer seeking to register a chemical substance (registrant) a right against
2 manufacturers, who have already registered such a substance, to access their testing data for tests
3 of the substance on animals. The rationale is to avoid unnecessary duplication of tests that have a
4 significant impact on our environment and cause unnecessary harm to animals (Recital 40). The
5 initial registrants shall receive a fair, transparent and non-discriminatory compensation for making
6 the testing data available to the potential registrant.

7 Data access rights may also follow from general doctrines of competition law. The basic
8 line of reasoning is that the aggregation of large datasets in the hands of a single market player may
9 constitute an abuse of a dominant position and would thus justify an interference with the rights of
10 the data holder for the benefit of the general public. In Europe, there is an extensive debate as to
11 whether this result can be achieved with the existing doctrines of competition law (for an overview
12 see Wolfgang Kerber, *Updating Competition Policy for the Digital Economy?*, 2019). The most
13 promising candidate is the so called ‘essential facilities doctrine’ (EFD), as it is designed to address
14 cases where a dominant market player refuses without objective justification to grant access to a
15 resource that is essential for a downstream market and thereby eliminates effective competition.
16 As the name suggests, the test was originally developed for cases of denied access to physical
17 facilities, such as ports. Later, the notion was expanded to cases where access to information was
18 denied based on IP-rights. With data being digitized information, the EFD seems to be very fitting
19 for cases of denied access to data. However, a closer look reveals that the requirements which have
20 been developed by the CJEU cannot easily be applied to situations of denied access (Heike
21 Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welker, *Modernisierung der*
22 *Missbrauchsaufsicht für marktmächtige Unternehmen*, 2018, p. 131 ff.; Jacques Crémer, Yves-
23 Alexandre de Montjoye and Heike Schweitzer, *Competition policy for the digital era*, 2019, p. 98
24 ff.; Furmann et al., *Unlocking digital competition*, Report for the Digital Competition Expert Panel,
25 2019, pp. 55 ff). Thus, some authors argue for a ‘fresh’ balancing of interests without regard to the
26 established confines of the EFD (Jacques Crémer, Yves-Alexandre de Montjoye and Heike
27 Schweitzer, *Competition policy for the digital era*, 2019, p. 98 ff). However, the main constraints
28 of competition law are its intervention threshold and intervention time. It is even in highly
29 concentrated markets, such as the markets for cloud service providers or B2C market platforms,
30 very difficult to prove the existence of a dominant market position under Article 102 TFEU.
31 Furthermore, competition law enforcement is time consuming and the relevant market might be
32 fundamentally transformed or potential innovative business models would have disappeared before
33 an ad-hoc competition case decision is validly taken and implemented (see Dirk Staudenmayer,
34 *Towards a European Private Law of the Digital Economy?*, in André Janssen and Hans Schulte-
35 Nölke (eds.), *Researches in European Private Law and Beyond*, 2020, p. 65, 84 ff). This is why it
36 has been argued that ex post competition law enforcement should be complemented with ex ante
37 regulation to prevent market tipping, ensure market contestability and stimulate innovation (see
38 Bertin Martens et al, *JRC Digital Economy Working Paper 2020-05, Business-to-Business data*
39 *sharing: An economic and legal analysis*, 2020, p. 35 ff).

40 Public interests play an even more significant role in B2G data sharing relationships. Access
41 to data is crucial when dealing with the growing number of societal challenges such as climate
42 change, natural disaster, urban planning or pandemics. One of the objectives the European
43 Commission plans to take forward in its Data Act (2021) is – besides the support of B2B data
44 sharing – to foster B2G data sharing for the public interest, especially in the light of the
45 recommendations of the report of the Expert Group on B2G Data Sharing (COM(2020) 66 final,
46 p. 12). In its final report, the Expert Group recommended the creation of an EU regulatory
47 framework providing a minimum level of harmonisation for B2G data-sharing processes (High-

1 Level Expert Group on Business-to-Government Data Sharing, Towards a European strategy on
2 business-to-government data sharing for the public interest – final report, 2020, p. 41 ff.). The
3 Expert Group’s proposed data-sharing requirements have some significant overlaps with the
4 approach chosen in Principles 24 ff. One of the main features the two approaches have in common
5 is their flexibility. The framework of the Expert Group should also apply without prejudice to the
6 applicable legal frameworks, e.g. for personal and non-personal data, and should further allow
7 Member States to choose rules compatible with their legislation or applicable to the specific sector.

8 The obligation to share data in the public sector is also discussed under ‘open government
9 data’ or ‘public-sector information’. The sharing of data between public bodies and private
10 enterprises (open government data) is regulated in the Open Data Directive (Directive (EU)
11 2019/1024) for EU institutions. Regarding research data, the OECD stated in 2006 that openness
12 means ‘access on equal terms for the international research community at the lowest possible cost,
13 preferably at no more than the marginal cost of dissemination’ (see OECD, Recommendation of
14 the Council concerning Access to Research Data from Public Funding, 2006, III.B.). Most
15 definitions of open data beyond research data include non-discriminatory access, costs of access,
16 and – in some cases – redistribution (see OECD, Enhancing Access to and Sharing of Data:
17 Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 41 f.). A prominent
18 example of a definition of open data can be found in the International Open Data Charter, which
19 defines open data as ‘digital data that is made available with the technical and legal characteristics
20 necessary for it to be freely used, re-used and redistributed by anyone, anytime, anywhere’
21 (International Open Data Charter, <https://opendatacharter.net/principles/>). See further Reporters’
22 Notes to Principle 25.

23 Justification plays a completely different role with regard to open government data. Rather
24 than look for a justification why open government data should be shared, governments need to
25 justify why data should not be shared (see Principle 1 of the International Open Data Charter,
26 <https://opendatacharter.net/principles/>). This is often simply expressed with the term ‘open by
27 default’, which is a general recognised principle of open government data (see Principles 1 and 3
28 of the G8 Open Data Charter signed at the G8 Summit on 18 June 2013; Recital 16 of Directive
29 (EU) 2019/1024). Typical exemptions to this rule are security or data protection concerns. See
30 further Reporters’ Notes to Principle 26.

31 **Principle 25: Granting of data access by the controller**

32 **(1) If the law affords a data access right within the meaning of Principle 24, the law should**
33 **provide that the controller must provide access under conditions that are fair,**
34 **reasonable and non-discriminatory within the class of parties that have been afforded**
35 **the right.**

36 **(2) Consistent with Principle 24(3), a data access right should be afforded only with**
37 **appropriate restrictions such as disclosure to a trusted third party, disaggregation,**
38 **anonymization or blurring of data, to the extent that affording the right without such**
39 **restrictions would be incompatible with the rights of others, or with public interests.**

1 **(3) The controller must comply with the duties under Principles 32 for the protection of**
2 **third parties, and restrictions under paragraph (2) must in any case enable the**
3 **controller to do so.**

4 **Comment:** *a. Relationship of Principles 24 and 25.* Principle 25 contains recommendations
5 for two important issues that should be addressed in a law of the sort described in Principle 24.
6 Both issues concern some of the essential duties a controller must fulfill when granting access to a
7 party seeking access to data on the basis of such a law. These recommendations may also be used
8 by courts as a source of supplementary principles for applying legislation that is silent as to these
9 points.

10 *b. Access under fair, reasonable, and non-discriminatory conditions.* Furthermore, the law
11 should provide that the controller must provide data access under conditions that are fair,
12 reasonable and non-discriminatory within the class of parties that have been afforded the data
13 access right. As noted above, this recommendation may also be used to supplement legislation that
14 is silent on this point, or where the law leaves the details to negotiations between the controller and
15 the recipient.

16 **Illustration:**

17 114. Where M in Illustration no. 112 grants access to vehicle data to R and the law does not
18 state how the remuneration to be paid by R is to be calculated, M must charge R fees
19 that are fair and reasonable, and must not charge R more than M charges other
20 independent repair shops in a comparable situation.

21 *c. Protection of others.* Consistent with Principle 20(2), Principle 25(2) provides that a data
22 access right should be afforded only with appropriate restrictions such as disclosure to a trusted
23 third party, disaggregation, anonymization or blurring of data, to the extent that affording the right
24 without such restrictions would be incompatible with the rights of others, or with public interests.
25 The public interest in encouraging the sharing of data for the benefit of innovation and growth may
26 in a given situation be in conflict with the legitimate interests of the controller itself or of third
27 parties. Those legitimate interests may follow from a variety of rights and considerations, ranging
28 from privacy to trade secrets protection to other secrecy concerns. Some of these interests may
29 equally amount to a public interest. While these Principles do not take a stand as to whether the

1 principle of ‘open by default’ or ‘privacy by default’ should generally prevail, Principle 25(2)
2 stresses the general necessity to tailor the modalities of any data access right to the legitimate
3 interests of others (i.e. the controller or any third party) such as by involving a data trustee or
4 escrowee within the meaning of Principle 13 and 14.

5 *d. Compliance with duties under Principle 32.* In a similar vein and consistent with
6 Principle 20(3), Principle 25(3) provides that the controller, when granting access to data to third
7 parties pursuant to a data right for the public interest, must comply with the general duties of a
8 supplier under Principle 32. This means that, even where access is not granted under a contract, the
9 controller must make sure that all restrictions that the controller itself must observe in the context
10 of data activities with regard to the data in question are imposed on the recipient. This may be
11 achieved by legal, institutional or technical means.

12 **Illustration:**

13 115. Where M in Illustration no. 112 grants access to vehicle data to R, M should have to
14 make sure it takes appropriate steps for the protection of, for example, trade secrets of
15 its suppliers or privacy concerns of other users of tractors. At least, M should have to
16 impose the same restrictions on R by way of a contract, and R should have to accept
17 this. However, this may not be sufficient. Rather, under Principle 32, M may need to
18 take further steps, including technical measures, such as allowing access and use of the
19 data only within a secure processing environment provided by M.

20 **REPORTERS’ NOTES:**

21 **U.S.:**

22 The ‘Open, Public, Electronic, and Necessary Government Data Act’ requires that open
23 Government data assets made available to the public pursuant to the Act must not be “encumbered
24 by restrictions, other than intellectual property rights ... that would impede the use or reuse of such
25 asset.” Open, Public, Electronic, and Necessary Government Data Act, Pub.L. 115–435, Title II,
26 Jan. 14, 2019, 132 Stat. 5534, sec. 202(a)(20).

27 **Europe:**

28 In Europe, the introduction of access rights to data, based on fair, reasonable and non-
29 discriminatory (FRAND) terms, has been discussed both on a policy and academic level for several
30 years (COM(2017) 9 final, p. 13; cf. Benoit Van Asbroeck et al., Building the European Data
31 Economy, Data Ownership – White Paper, 2017). FRAND-based access was originally introduced
32 as a remedy in competition law cases to ensure the supply of a particular product or the access to

1 specific infrastructure. For example, in the Microsoft Case, Microsoft was ordered to disclose
2 interoperability information, which was indispensable for producing programs that are compatible
3 with Windows, on a non-discriminatory basis and under terms that are reasonable in order to
4 remedy distortions of competition (European Commission Case COMP/C.3/37.792, 24. Paras.
5 1005-1008 – Microsoft, 24 March 2004). FRAND terms also play an important role in the licensing
6 of Standard Essential Patents (SEPs), which may cover standard specifications that are essential
7 for facilitating innovation and a level playing field in the ICT sector. Industry stakeholders, who
8 invested in the creation and protection of these standards, of course, have an interest in receiving a
9 return on this investment by way of licensing. However, exclusive rights conferred by patents may
10 defeat the benefits of having industry-wide standards that are available for public use. To strike a
11 balance between these two competing interests, SEP holders are required to license their SEPs on
12 FRAND terms (Y Ménière, ‘Fair, Reasonable and Non-Discriminatory (FRAND) Licensing
13 Terms: Research Analysis of a Controversial Concept,’ 2015). It has been proposed, that the
14 findings of the CJEU in the *Huawei* Case (CJEU Case C-170/13 ECLI:EU:C:2015:477 – *Huawei*)
15 on a negotiation framework for the licensing of SEP on FRAND terms, could be used as inspiration
16 for cases of data access (see Josef Drexl, *Designing Competitive Markets for Industrial Data -*
17 *Between Propertisation and Access*, [2017] JIPITEC 257, 285). Thus it could assist the parties to
18 reach an agreement on the price of access (see Thomas Tombal, *Economic dependence and data*
19 *access*, [2020] *International Review of Intellectual Property and Competition Law* 51:70, 94 f).

20 Especially in Communications from the European Commission, data access rights based on
21 FRAND terms have repeatedly been discussed as an instrument to address market failures in the
22 data economy (COM(2017) 9 final, p. 13; COM(2020) 66 final, p 13). Some variations of the
23 FRAND principle can be found in connection with sector-specific access rights. For example, the
24 car manufacturer, who according to Article 61 Type Approval Regulation (Regulation (EU)
25 2018/858) must disclose technical information to independent repair service providers (see
26 Reporters’ Notes to Principle 24), ‘may charge reasonable and proportionate fees for access’.
27 Under the REACH Regulation (Regulation (EC) No 1907/2006), the registrant of a chemical
28 substance must share data regarding tests on vertebrate animals with potential registrants.
29 According to Article 27(3), ‘the previous registrant and potential registrant(s) shall make every
30 effort to ensure that the costs of sharing the information are determined in a fair, transparent and
31 non-discriminatory way’.

32 FRAND-based access rights can also be found in the Regulation that established rules for
33 the participation in the European Union’s Framework Programme for Research and Innovation
34 (Horizon 2020) (Regulation 1219/2013). Article 48(1) grants participants in the Framework
35 Programme an access right to the results of another participant in the same action if those results
36 are needed by the former to exploit its own results. Subject to an agreement, this access shall be
37 granted under fair and reasonable conditions (Article 48(2)). In Article 2(10) ‘fair and reasonable
38 conditions’ are defined as ‘conditions, including possible financial terms or royalty-free conditions,
39 taking into account the specific circumstances of the request for access, for example the actual or
40 potential value of the results or background to which access is requested and/or the scope, duration
41 or other characteristics of the exploitation envisaged.’

42 In the proposed Data Governance Act (DGA, COM(2020) 767 final), FRAND is a condition
43 for providing data sharing services. Article 11(3) stipulates that the provider of data sharing
44 services needs to ‘ensure that the procedure for access to its service is fair, transparent and non-
45 discriminatory for both data holders and data users, including as regards prices’.

46 Finally, the recent proposal for a Digital Markets Act (COM(2020) 842 final) obligates
47 gatekeepers to provide to any third party providers of online search engines, upon their request,

1 access to ranking, query, click and view data in relation to free and paid search generated by end
2 users on online search engines of the gatekeeper, on a FRAND basis.

3 **Principle 26: Data activities by recipient**

4 **(1) If the law affords a data access right within the meaning of Principle 24 to a party, the**
5 **law should provide that, subject to paragraph (2), the party may utilize the data it**
6 **receives in any lawful way and for any lawful purpose that is not inconsistent with**

7 **(a) the public interest for which the right was afforded, provided the recipient had**
8 **notice of that interest;**

9 **(b) restrictions for the protection of others imposed under Principle 25(2); or**

10 **(c) any agreement between the parties, including an agreement concerning duties and**
11 **restrictions imposed by the controller on the recipient under Principle 32.**

12 **(2) A party to whom a data access right is afforded under Principle 24 may not utilize that**
13 **data in a way that harms the legitimate interests of the original controller more than is**
14 **inherent in the purpose for which the right was afforded.**

15 **Comment:** *a. Freedom of use as the default rule.* While Principle 25 sets out basic
16 principles governing the controller's duties, Principle 26 sets out principles governing the recipient
17 of the data and any data activities this recipient may engage in. Where the law imposes a data
18 access right within the meaning of Principle 24 (or an equivalent data sharing obligation) it could
19 provide either that the data may be used exclusively for the purposes for which the right had
20 originally been afforded, or the law can be more liberal with regard to data use. This Principle
21 recommends that the law should take the latter approach, stating that the recipient may use the data
22 in any lawful way and for any lawful purpose as long as this is consistent with a number of
23 limitations originating either from the law or from the agreement of the parties. This approach is
24 more 'open' and may better help foster innovation and growth. This is also consistent with Principle
25 7(2)(c)(iv), which, for data supply contracts, opts for a 'sales approach' rather than for a 'license
26 approach'. Thus, this Principle opts for freedom of use as the default rule.

1 *b. Limitations on freedom of use.* The data access rights provided for in paragraph (1) must
2 be exercised consistent with three limiting factors. First, the data received may be used only for a
3 purpose that is not inconsistent with the public interest for which the right was afforded. For data
4 use to be inconsistent with the public interest it must actually contravene or undermine that public
5 interest. It is not enough that the type of data use just failed to be contemplated by the legislator
6 when the access right was created.

7 **Illustration:**

8 116. Municipality M is under a statutory obligation to make data from smart road
9 infrastructure freely available. The stated purpose of the statute is to enable businesses
10 to develop smart services for the improvement of the traffic situation. Business B uses
11 the data for developing a service that helps steer smart home equipment, causing air
12 conditioning facilities of premises to stop importing outside air when nearby traffic is
13 dense. This is not a purpose foreseen when the access right was created, and the access
14 right would probably not have been created for that purpose. But, as this innovative use
15 is not explicitly excluded by the relevant statute, and is not inconsistent with the original
16 purpose (and does not harm M, see paragraph (2)), B should be allowed to use the data
17 for this purpose.

18 However, there are usually also more specific limitations, either imposed directly by the
19 law that affords the access right (see Principle 25(2)) or individually by the controller under an
20 agreement between the controller and the recipient, including an agreement made to ensure that the
21 requirements of Principles 25(3) and 32 are met.

22 **Illustration:**

23 117. Municipality M in Illustration no. 116 makes data that indicates traffic density and the
24 speed at which vehicles are going available to research institute R. In the light of the
25 fact that the data includes IP-addresses of connected vehicles, it would theoretically be
26 possible to create mobility profiles for particular vehicles with the data, which, if
27 combined with other data, could be rather sensitive information whose disclosure might
28 harm the legitimate interests of third parties. This is why M makes the data available
29 only under quite strict conditions, including restrictions on how the data must be stored
30 securely and for what types of purposes they may be used. These conditions might

1 already be listed in a law regulating the granting of data access by M, or may be imposed
2 by M on R on a contractual basis in the individual case. R is bound by these conditions.

3 *c. No-harm principle.* Situations may arise where the party benefiting from an access right
4 under Principle 24, or an equivalent data sharing obligation, uses the data in a way that harms the
5 legitimate interests of the original controller. What counts as ‘harm[ing] the interests of the original
6 controller’ should be answered according to general principles, taking into account that inflicting
7 harm on third parties within that controller’s sphere of interest may amount to harm inflicted on
8 the controller itself. In many cases, this is almost inevitable, such as where the original controller
9 and the party receiving data are competitors and thus the latter party’s competitive gain is mirrored
10 by the original controller’s competitive loss. However, where the receiving party uses the data to
11 cause harm to the original controller that goes beyond what is inherent in the purpose for which
12 data sharing was introduced, this violates, at the least, principles of fundamental fairness. It should
13 therefore be prohibited. This is without prejudice to paragraph (1), i.e. where harming the interests
14 of the original controller is already inconsistent with the public interest for which the data access
15 right was afforded, or with additional limitations imposed by the law or by agreement, it may
16 already be prohibited under paragraph (1).

17 **Illustrations:**

18 118. Under an open research data scheme, research institute R1 is obligated to make
19 research data freely available. Research institute R2 uses the data to advance its own
20 research, saving millions in investment, and gains a decisive competitive edge over R1
21 in a competition for public funds. Use of the data by R2 harms the interests of R1, but
22 this harm is inherent in the purpose for which the obligation to share research data was
23 imposed, so R2 is not acting in violation of Principle 26(2).

24 119. In a situation such as that in Illustration no. 118, research institute R2 uses the research
25 data published by R1 to prove that R1 has forged research results, pretending to have
26 actually run laboratory trials that were really just simulated by a computer. The
27 detection of research fraud is within the range of purposes of open research data
28 regimes, so R2 is not acting in violation of Principle 26(2).

1 two decades (see COM(1998) 585 final and Public Sector Information (PSI) Directive
2 2003/98/EC). The underlying rationale is that government data is an untapped resource for
3 innovative products and services that has been produced with public money. Therefore, the data
4 should be publicly available and used for the benefit of society. With the Open Data Directive
5 (Directive (EU) 2019/1024) the European legislator renewed its open data efforts and introduced
6 new rules to facilitate the re-use of data held by the public sector. An additional set of provisions
7 for the re-use of specifically protected data held by public bodies (such as personal data), which is
8 largely excluded from the scope of the Open Data Directive, has been proposed by the European
9 Commission in the Data Governance Act (COM(2020) 767 final). The notion that public data
10 should be open by default is not only promoted by the European Union but has, for example, also
11 been recommended by the OECD. To maximize the use and re-use of public data, member
12 countries should assume openness in public sector information as a default rule wherever possible.
13 Grounds for limitations of this principle may be the protection of national security interests,
14 personal privacy or the preservation of private interests, for example where protected by copyright
15 (OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public
16 Sector Information, 2008). Similarly, in the G8 Open Data Charter, the members of the G8 declared
17 that free access to, and subsequent re-use of, public data are of significant value to society and the
18 economy. They agreed to orient their governments towards open data by default while recognizing
19 that there are legitimate reasons, such as intellectual property and data protection law, that may
20 restrict the sharing of data. Further, they agreed that data should be available free of charge in order
21 to encourage its most widespread use and be released in open formats wherever possible, to ensure
22 that the data is available to the widest range of users for the widest range of purposes. In a similar
23 vein, Principle 1 of the International Open Data Charter, a collaboration between over 100
24 governments and organizations, states that there should be a presumption of publication for
25 government data and that governments should justify data that is kept closed, for example for
26 security or data protection reasons.

27 While the data openness debate was for a long time primarily focused on public data,
28 facilitating the exchange of data has also become a policy objective for B2B relations. With markets
29 becoming more and more data driven, having access to data may not only determine economic
30 success in the digital age but is also essential to create innovative services and products, reduce
31 costs and improve efficiency. Triggered by new technological developments, such as IoT and AI,
32 openness of data in the private sector has moved to the center of European policy discussions. It is,
33 however, recognized that open data, the most extreme approach to data openness, may be less
34 fitting for privately held data than for public data and thus different considerations need to be taken
35 into account. (OECD, Enhancing Access to and Sharing of Data: Reconciling risks and benefits of
36 data re-use, 2019). Given the potential benefits of data openness, the new college of the European
37 Commission has set out to create a framework that enhances the data flow between businesses. A
38 first step in this direction has been taken by the Data Governance Act (COM (2020) 767 final),
39 which not only contains rules on the re-use of public data but also proposes provisions to facilitate
40 the sharing of data among businesses. Further measures are planned to be put forward in 2021 by
41 the Data Act.

42 The data exchange between businesses and governments (B2G) is guided by the principle
43 of ‘purpose limitation’ (or ‘data-use limitation’) (COM(2018) 232 final , p. 13). This principle
44 states that the use of private sector data should be clearly limited to one or more purposes to be
45 specified as clearly as possible in the contractual provisions that establish the B2G collaboration.
46 These may include a limitation of duration for the use of the data. Furthermore, the private sector
47 entity should receive specific assurances that the data obtained will not be used for unrelated

1 administrative or judicial procedures. The High-Level Expert Group on B2G Data Sharing
 2 essentially upheld the core tenet of the principle but proposed to clarify that the public sector should
 3 be able to combine the private-sector data with data from other sources. Furthermore, it was
 4 suggested to change the term to ‘data-use limitation’, because ‘purpose limitation’ is primarily used
 5 in a privacy law context (HLEG on B2G Data Sharing, Towards a European strategy on business-
 6 to-government data sharing for the public interest, 2020).

7 By recommending that data may be used for any lawful purpose and in any lawful way
 8 unless it is explicitly agreed or stated otherwise or inconsistent with the purpose for which the right
 9 had originally been afforded, Principle 26 follows the general trend of promoting data openness in
 10 the B2B sector, in order to help foster innovation and growth.

11 *c. No-harm principle.* The meaning of the ‘no-harm’ principle formulated in Paragraph 2
 12 does not correspond with that of the ‘do no harm’ principle for B2G data sharing which has been
 13 put forward by the European Commission (COM(2018) 232 final, p. 13). The meaning the
 14 European Commission attached to the principle of ‘do no harm’ is that B2G data collaborations
 15 must ensure that protected interests, such as trade secrets, are respected. While Principle 26(2) also
 16 concerns the protection of such interests, its scope is limited to the legitimate interests of the
 17 original controller and parties within that controller’s sphere of interest. The interests of protected
 18 third parties are dealt with in Part IV of these Principles. The conflict in terminology between this
 19 Principle and the B2G principles of the European Commission might soon be resolved, as the
 20 HILEG on B2G data sharing suggested changing the ‘do no harm’ principle to ‘risk mitigation and
 21 safeguards’. The general notion of fairness that the freedom to use a resource may not
 22 inappropriately harm the interests of others – under the same term but in a very different context –
 23 can also be found in international environmental law. According to the Rio Declaration on
 24 Environment and Development 1992, states have the right to exploit their own resources in
 25 accordance with their own environmental and developmental policies, but they must ensure that
 26 activities within their jurisdiction or control do not cause damage to the environment of other States
 27 or of areas beyond the limits of national jurisdiction.

28 Principle 27: Reciprocity

29 **If the law affords a data access right within the meaning of Principle 24 to a party against**
 30 **a controller, this is a strong argument for affording a similar data access right to the**
 31 **original controller against the first party under comparable circumstances. Whether**
 32 **this argument should prevail depends, inter alia, on whether affording such a reciprocal**
 33 **right would be inconsistent with the purpose of provision of access to the first party.**

34 **Comment:** *a. Reciprocity.* This Principle is a very ‘soft’ Principle, reflecting basic notions
 35 of fundamental fairness and giving some – necessarily general – guidance as to their possible
 36 implementation. Generally speaking, notions of fairness require a certain degree of reciprocity, i.e.
 37 where a party benefits from receiving data under a data sharing regime for the public interest, that
 38 party should normally be prepared to share similar data under similar conditions with the controller

1 that had originally shared the data. This may often be achieved by simply formulating the scope of
2 the relevant law in a way that it imposes the same duties on the recipient.

3 **Illustration:**

4 122. In a situation such as that in Illustration no. 118, research institute R2 should normally
5 be subject to the same open research data regime as R1. As a result, next time it may be
6 R1 that profits from data published by R2.

7 In many situations, however, more sophisticated steps may need to be taken in order to
8 provide for reciprocity, e.g. because the original controller and the receiving party are very different
9 and not subject to the same rules.

10 **Illustration:**

11 123. The law provides that a municipality must share, for free, mobility data from smart
12 road infrastructure with whoever is interested in the data. When designing the law, the
13 legislator might wish to consider including a duty on recipients that gain valuable
14 insights from this data, e.g. about traffic flows in the city, to share this derived or
15 inferred data with the municipality.

16 Naturally, reciprocity is not called for where the purpose for which the access right within
17 the meaning of Principle 24 was originally afforded is inconsistent with reciprocity, such as where
18 the data access right was afforded under some State's domestic law in order to balance an initially
19 imbalanced market position of the parties.

20 **Illustration:**

21 124. If the law provides for a data sharing obligation for large platforms for the benefit of
22 MSMEs trying to enter the market it would obviously undermine the purpose of that
23 law if, conversely, and relying on the notion of reciprocity, the large platforms could
24 exercise a data access right against the MSMEs.

25 **REPORTERS' NOTES:**

26 **U.S.:**

27 For a discussion of reciprocity in data sharing systems, see, e.g., Institute of International
28 Finance, Reciprocity in Customer Data Sharing Frameworks (July 2018), available at
29 https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_fra

1 neworks_20170730.pdf. See also Congressional Research Service, Cross-Border Data Sharing
2 Under the CLOUD Act ((2018); De Wolf, V., Sieber, J., Steel, P., & Zarate, A. (2005). Part I: What
3 Is the Requirement for Data Sharing? IRB: Ethics & Human Research, 27(6), 12-16.
4 doi:10.2307/3563537

5 **Europe:**

6 In European legislation on data sharing, an explicit reference to the notion of reciprocity
7 can be found in the INSPIRE Directive (Directive 2007/2/EC). Article 17 of the INSPIRE Directive
8 provides rules for the sharing of spatial data between public authorities of Member States for the
9 purposes of public tasks that may have an impact on the environment. Any restrictions likely to
10 create practical obstacles to the sharing of spatial data sets and services are precluded. Charge fees
11 for and licensing of the spatial data remains possible but should be kept to the minimum required
12 to ensure the necessary quality and supply of spatial data sets and services together with a
13 reasonable return on investment. The INSPIRE Directive explicitly stipulates that, on the basis of
14 reciprocity and equivalence, the regime put forward by Article 17(1) – (3) shall also be open to
15 bodies established by international agreements to which the EU and Member States are parties for
16 tasks that may have an impact on the environment.

17 Another explicit reference to the principle of reciprocity in data exchanges can be found in
18 connection with ambient air data. In an Implementing Decision, the European Commission lays
19 down rules for the reciprocal exchange of ambient air quality data between Member States, in order
20 to establish a sound informational basis for measures to reduce air pollution (Commission
21 Implementing Decision 2011/850/EU OJ L 2011/335, p 86).

22 The idea underlying Principle 27 is already, to some extent, present in patent law. The
23 predominant example is Article 31 TRIPS which addresses other use without authorization of the
24 right holder and sets out in its paragraph (l) that where such use is authorized to permit the
25 exploitation of a patent ('the second patent') which cannot be exploited without infringing another
26 patent ('the first patent'), the owner of the first patent shall be entitled to a cross-licence on
27 reasonable terms to use the invention claimed in the second patent (see also Section 24(2) German
28 Patent Act). In addition, the typical FRAND declarations on standard-essential patents offer the
29 holder the option of granting a FRAND licence only on the condition of reciprocity (see ETSI IPR
30 Policy para 6.1).

31 **Part IV: Third Party Aspects of Data Activities**

32 **Chapter A: Protection of Others against Data Activities**

33 **Principle 28: Wrongfulness of data activities vis-à-vis another party**

34 **(1) Data activities are wrongful vis-à-vis another party (a 'protected party') if:**

35 **(a) they interfere with any right of the protected party that has third-party effect per**
36 **se within the meaning of Principle 29;**

1 **(b) they do not comply with contractual limitations on data activities, enforceable by**
2 **the protected party, of the sort described in Principle 30; or**

3 **(c) access to the data has been obtained from the protected party by unauthorized**
4 **means within the meaning of Principle 31.**

5 **(2) In assessing whether data activities are wrongful, the conditions under which these**
6 **activities are pursued, such as provision of an adequate level of data security or**
7 **compliance with any duty under Principle 32, should be taken into account.**

8 **(3) Implementation of this rule should take into account applicable doctrines of**
9 **justification, such as freedom of information and expression.**

10 **Comment:** *a. General observations.* Previous Parts of these Principles have focused on
11 legal relationships that are essentially bilateral in nature. Even where contracts are of a type that is
12 usually concluded among multiple parties, such as data pooling arrangements, the relevant
13 Principles in Part II have focused on the relationship among the contracting parties. Likewise, even
14 when data rights are of a type usually exercised by many parties in parallel, such as rights to receive
15 an economic share in profits derived, the relevant Principles in Part III have focused on the
16 relationship between a party exercising a data right and the controller against whom the right is
17 exercised. Rights and legitimate interests of third parties play a role, of course, such as with regard
18 to certain due diligence and data security obligations (e.g. Principle 7(2)(c)(iv)), or in the context
19 of the factors that need to be assessed when deciding whether or not to grant a data right (e.g.,
20 Principle 19(2)(c)), and if so, which specifications should be made and which protective measures
21 for the benefit of affected parties should be taken (e.g., Principle 19(3)). However, in those contexts
22 the legitimate interests of affected parties were considered as factors to be taken into account within
23 a wider balancing exercise, not as rights which those affected (third) parties might themselves
24 enforce against the contracting parties or the party exercising a data right and the controller.

25 This is where Part IV comes into play. Chapter A of Part IV gives guidance to courts and
26 legislators as to when data activities should be considered wrongful vis-à-vis another party, be that
27 a third party or even a contracting party (as a contracting party may, where data is passed on in a
28 chain of transactions, become a third party with regard to a downstream transaction). The term
29 ‘data activities’ is defined very broadly and covers any activity with regard to data, including
30 acquisition, control, processing or use, and onward supply. While Chapter A sets out the general

1 grounds for wrongfulness vis-à-vis a protected party, Chapter B more specifically deals with the
2 situation of onward supply of data and the effects such onward supply may have on the protection
3 of affected parties. In this context, Chapter B not only states duties for the onward supply of data
4 (Principle 32), but also sets out conditions under which an initial supplier may take direct action
5 against a downstream recipient (Principle 33), and the conditions under which wrongful activities
6 on the part of a supplier also make the activities of a downstream recipient wrongful (Principle 34).
7 Chapter C addresses similar issues in the context of processing of data.

8 Principle 28 is of an introductory nature. It sets out three grounds of wrongfulness of data
9 activities that are described in more detail in Principles 29 to 31. The list provided in Principle
10 28(1) is not exhaustive, i.e. there are other reasons why an activity with regard to data may be
11 wrongful, the most obvious of these being that it is violating law other than law referred to in
12 Principles 29 to 31 or is generally in breach of contract, in particular a contract described in Part
13 II. Of course, as stated in Principle 1(2), nothing in Principles 28 to 37 is intended to amend or
14 create data privacy or data protection law, intellectual property law, or trade secret law, so if any
15 of these bodies of law provides for different or more specific solutions for the issues addressed in
16 Part IV, these solutions take priority.

17 *b. Grounds of wrongfulness.* There are three cases where a data activity is considered to be
18 wrongful under the non-exhaustive list in paragraph (1). The first case is interference with any right
19 within the meaning of Principle 29, i.e. intellectual property rights or personality rights such as
20 data privacy/protection rights.

21 **Illustration:**

22 125.Provider B of a video game processes user data covered by a data protection regime
23 that requires, for processing to be lawful, the users' consent. If B processes the data
24 without such consent these data activities are wrongful vis-à-vis the data subjects within
25 the meaning of Principles 28(1)(a) and 29.

26 The second case is non-compliance with contractual limitations within the meaning of
27 Principle 30. While the breach of any contractual duty may give rise to remedies under applicable
28 law, it is more specifically the breach of a contractual duty limiting data activities that leads to
29 wrongfulness under Principle 28(1)(b). Such contractual limitations not only lead to wrongfulness

1 vis-à-vis the contracting partner, but may also, under the conditions set out in Principle 34, take
2 effect vis-à-vis a downstream recipient.

3 **Illustration:**

4 126. Controller C of valuable sensor data entrusts the data to processor P. The contract with
5 P contains a clause according to which P may not pass the data on to any third party. If
6 P, in violation of that clause, passes the data on to T, this data activity of P is wrongful
7 vis-à-vis B under Principles 28(1)(b) and 30. Whether T is also acting wrongfully
8 depends on Principle 34.

9 127. Controller C of the sensor data sells the data to business B under a contract. The data
10 is immediately transferred to B, and B is under an obligation to pay the purchase price
11 in several installments. After B has failed to pay two installments despite reminders, C
12 terminates the contract. B is clearly in breach of contract, and after termination of the
13 contract B must erase the data (cf. Principle 4(2)) and may no longer use it, but this is
14 not the kind of ‘contractual limitation’ addressed by Principles 28(1)(b) and 30.

15 Finally, data activities are wrongful according to Principle 28(1)(c) if data has been
16 obtained by unauthorized means within the meaning of Principle 31. This concerns primarily the
17 relationship between the person that obtained the data by unauthorized means and the initial
18 controller (from which this person obtained the data). Whether this ground of wrongfulness also
19 takes effect against a downstream recipient is determined by Principle 34.

20 **Illustration:**

21 128. If hacker H hacks B’s servers in Illustration no. 125 and thus obtains access to the user
22 data, that is certainly a wrongful data activity under Principles 28(1)(c) and 31. If H
23 passes the data on to T the question of whether T is also acting wrongfully is a question
24 of Principle 34.

25 *c. Data security and other additional standards.* Paragraph (2) clarifies that rightfulness of
26 data activities is not just a matter of whether control, a particular form of processing or onward
27 supply is rightful as such, but also a matter of how it takes place. A particularly important
28 requirement is that of providing an adequate level of data security. It is beyond the scope of these
29 Principles to define which technical measures need to be taken, and what qualifies as an adequate

1 level of security. These determinations can be made in specific legislation or industry standards or,
2 in their absence, be reached by courts relying on general doctrines and principles considering the
3 weight of the rights of third parties that are at stake, the magnitude of the risk of data breaches
4 occurring, and the gravity of the potential consequences. Failure to comply with these requirements
5 leads to wrongfulness of the data activities.

6 **Illustration:**

7 129.If B in Illustration no. 125 has obtained the users' consent but fails to apply basic data
8 security measures when storing the data, storage of the data (as a type of data activity)
9 may be wrongful vis-à-vis the data subjects.

10 Apart from the requirement to provide an adequate level of data security there may be a
11 host of other requirements, such as requirements under applicable rules of public law, and of course
12 any duty to be complied with in the context of onward transfer under Principle 32.

13 *d. Justifications.* As Principle 28 is largely founded on a tort law logic, due account must
14 be taken of possible grounds of justification. One example would be freedom of the press, such as
15 where investigative journalists obtain control of particular data.

16 **Illustration:**

17 130.Journalist J receives bank account data proving that politician P has misappropriated
18 public funds. Even if J has notice that this data has been acquired either in breach of
19 contract or by unauthorized means, J's own data activities may exceptionally be
20 justified and therefore not wrongful according to Principle 28(3).

21 **REPORTERS'NOTES:**

22 **U.S.:**

23 There are many circumstances under U.S. contract law in which an action that is in breach
24 of contract as between the parties is wrongful with respect to a third party, who then has redress
25 for that breach. Sometimes, the circumstances are provided for by statute. See, e.g., UCC § 2-318,
26 providing that a seller's warranty extends to certain third parties. Other times, common law
27 doctrines, particularly those relating to third-party beneficiaries, bring about a similar result. See
28 generally Restatement (Second) Contracts, Chapter 14.

29
30 Third party effects in tort law can be seen, *inter alia*, in the field of products liability. See,
31 e.g., Restatement (Third) of Torts: Products Liability § 1.
32

1 See also Stefan Bechtold, Digital Rights Management in the United States and Europe, 52
2 Am. J. Comp. L. 323 (2004).

3 Europe:

4 *a. General observations.* In EU law, a line is drawn between rights that can only be enforced
5 against a certain party ('*inter partes* rights', 'relative rights') and rights that can be enforced against
6 everybody ('*erga omnes* rights', 'absolute rights' or 'rights with third-party effects'). The most
7 prominent example for the former is rights arising out of contractual relationships. As a general
8 rule, third parties can neither acquire rights from the contract nor are they obligated to adhere to
9 the obligations stated in the contract, as the contractual relationship only produces effect for the
10 contracting parties. The relative effect of contractual rights is a central notion in European contract
11 law and is explicitly stated in Article 1165 French Civil Code which articulates that 'agreements
12 produce effect only between the contractual parties'. However, there are some exceptions to this
13 general rule. For example, it is prohibited to deliberately induce a person not to fulfil the person's
14 contractual obligations towards the other party to the contract. In such circumstances, the person
15 inducing the non-performance may be considered as committing a tort/delict (see Article VI –
16 2:211 DCFR; Article 2:211 Principles of European Law – Non-Contractual Liability Arising out
17 of Damage Caused to Another (PEL Liab. Dam.); Reporters' Notes to Principle 34). Absolute
18 rights on the other hand can be enforced against any third party. The most relevant examples of
19 such rights with regard to data can be found in copyright law, the *sui generis* protection of databases
20 and in the GDPR (see Reporters' Notes to Principle 29).

21 *b. Grounds of wrongfulness.* The grounds of wrongfulness draw some inspiration from the
22 Trade Secrets Directive (Directive (EU) 2016/943), under which the use or disclosure of a trade
23 secret is considered unlawful if carried out by a person who unlawfully acquired the trade secret,
24 or is in breach of a confidentiality agreement, contractual duty or any other duty that limits its
25 disclosure or use (Article 4(3) Trade Secrets Directive). The acquisition of a trade secret without
26 the consent of the trade secret holder is considered unlawful, whenever carried out by unauthorised
27 access to, appropriation of, or copying of any documents, objects, materials, substances or
28 electronic files, lawfully under the control of the trade secret holder, containing the trade secret or
29 from which the trade secret can be deduced. Furthermore, the acquisition of a trade secret is
30 unlawful if it is carried out by any other conduct which, under the circumstances, is considered
31 contrary to honest commercial practices (Article 4(2) Trade Secrets Directive). The protection
32 under the Trade Secrets Directive is nearly identical to the protection of undisclosed information
33 in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)
34 between all the member nations of the World Trade Organization (WTO).

35 *c. Data security and other additional standards.* The GDPR (Regulation (EU) 2016/679)
36 qualifies processing in a manner that ensures appropriate security of the personal data as one of the
37 guiding principles relating to processing of personal data (see Article 5(1)(f) GDPR). This includes
38 the protection against unauthorized or unlawful processing and against accidental loss, destruction
39 or damage by using appropriate technical or organizational measures. This principle influenced, in
40 particular, Article 6(4) GDPR, which lays down the conditions under which the controller is
41 entitled to process personal data for a purpose other than that for which the personal data were
42 collected. In assessing whether such processing is lawful, account must be taken of the existence
43 of appropriate safeguards for both the original and intended further processing (see also Recital 50
44 GDPR). Finally, a high level of security for the storage and transmission of non-personal data is
45 also a condition for providing a data sharing service in the recent proposal for a Data Governance

1 Act (DGA, Article 11(8) COM(2020) 767 final). The failure to comply with the conditions in the
2 DGA can lead to financial penalties or even the forced cessation of the data sharing service.

3 The standards for cybersecurity, network and information security are currently being
4 developed all around the world (for an overview see European Commission, Rolling Plan for ICT
5 Standardisation, 2020, p. 34 ff.). This includes work from international standardisation agencies
6 such as the CEN CENELEC Joint Technical Committee on ‘Cybersecurity and data protection’
7 (CEN-CLC/JTC 13) and the European Telecommunications Standards Institute (ETSI), e.g. in the
8 Technical Committee Cyber (TC Cyber). On a European level, ENISA (European Cybersecurity
9 Agency) drafted a candidate cybersecurity certification scheme on the basis of the Cybersecurity
10 Act. Furthermore, the International Organisation for Standardisation (ISO) works on several areas
11 of information- and cybersecurity in its Sub Committee 27 (SC 27, see
12 <https://www.iso.org/committee/45306.html>). Further initiatives are pursued by the International
13 Telecommunications Union and the Internet Engineering Task Force (IETF).

14 *d. Justification.* Under tort law, liability is excluded, if the defendant’s actions are justified.
15 Examples of widely recognized grounds of justification can be found, for example, in the Principles
16 of European Tort Law (PETL): the defendant acts in self-defence, under necessity, because the
17 help of the authorities could not be obtained in time (self-help), with the consent of the victim, or
18 by virtue of lawful authority (cf. Art. 7:101 PETL). These defences are also laid down in Chapter
19 5, Book VI of the Draft Common Frame of Reference (DCFR) and the Principles of European Law
20 (PEL).

21 Liability under the Trade Secrets Directive is excluded where the alleged acquisition, use
22 or disclosure of the trade secret was carried out (a) to exercise the right to freedom of expression
23 and information as set out in the Charter, including respect for the freedom and pluralism of the
24 media; (b) to reveal misconduct, wrongdoing or illegal activity, provided that the respondent acted
25 for the purpose of protecting the general public interest; (c) by workers for their representatives as
26 part of the legitimate exercise by those representatives of their functions in accordance with
27 European Union or national law, provided that such disclosure was necessary for that exercise; and
28 (d) for the purpose of protecting a legitimate interest recognised by European Union or national
29 law. However, the broader formulation chosen in Principle 28(3) allows a more flexible approach
30 that allows for new grounds for justification that may arise in the future.

31 The GDPR leaves the relationship between the right to the protection of personal data and
32 the right to freedom of expression and information, including processing for journalistic, academic,
33 artistic or literary purposes, to the law of the Member States. Member States shall provide for
34 exemptions or derogations if they are necessary to reconcile the right to the protection of personal
35 data with the freedom of expression and information (Article 85).

36 **Principle 29: Rights that have third-party effect per se**

37 **(1) For the purpose of Principle 28(1)(a), rights that have third-party effect per se include**
38 **the following:**

39 **(a) intellectual property rights and similar rights;**

40 **(b) data privacy/data protection rights and similar rights; and**

1 (c) any other rights that, under the applicable law, have similar third-party effects.

2 (2) The extent to which rights within the meaning of paragraph (1) limit data activities, as
3 well as the effect of such limitations, is determined by the applicable law.

4 **Comment:** *a. Traditional erga omnes rights.* Principle 29 provides a non-exhaustive list of
5 rights that take effect against any third party (*erga omnes*), as contrasted with rights that take effect
6 only against a particular party (*inter partes*). What is special about the rights listed in Principle 29
7 (compared, e.g., with entitlements following from situations described in Principles 30 or 31) is
8 that these rights have third-party effect per se, and others have to respect them per se, and
9 infringements are normally wrongful, subject to justification, without additional elements such as
10 bad faith (even though the applicable national law may, of course, impose such additional elements
11 for there being a remedy for infringement).

12 Rights that take effect against any third party in this way include intellectual property rights
13 (paragraph (a)), such as patent protection or copyright protection, including protection for computer
14 programs. Data may be protected by such IP rights, but not all data is IP protected, and, in fact,
15 most data is probably not. Apart from IP rights, there is also a number of rights that are closely
16 related to IP rights, because they work in a similar manner. An example for such a related right
17 would be the European *sui generis* database right under Directive 96/9/EC, which is a particular
18 form of investment protection.

19 Besides intellectual property rights there are a number of entitlements with regard to data
20 that do have third-party effect but work in a different manner. This concerns, in particular,
21 personality rights, which are the basis of data privacy/data protection rights under a number of legal
22 regimes (paragraph (b)). The extent to which such rights are vindicated under the relevant legal
23 regimes by way of public enforcement or private enforcement is not determinative, as long as the
24 basis for public enforcement still is the protection of particular parties (as contrasted with, for
25 example, the market).

26 **Illustration:**

27 131. Assume that the law in a U.S. State has adopted a data privacy regime that does not
28 provide for rights that individual data subjects, or a class of data subjects collectively,
29 can exercise and enforce in court, but that provides only the basis for State authorities
30 to take action against a business. Provided the law was introduced to protect data

1 subjects, the protection thus afforded would still potentially qualify as a ‘right’ within
2 the meaning of Principle 29. Where, however, the rationale was the regulation of data
3 markets this would fall outside the scope of Principle 29.

4 Principle 29(1)(c) is not exhaustive and thus leaves room for rights that, under the
5 applicable law, have similar third-party effects. A third-party effect can be considered as ‘similar’
6 where, by effect of law, any third party interfering with the right might face remedies and other
7 sanctions. This will often include trade secrets, which are not intellectual property, but which, due
8 to a separate body of law affording protection, provide their holder with a kind of ‘soft IP
9 protection’. Whether or not this is the case under the applicable law depends, in particular, on
10 whether or not a third party buying a trade secret in good faith from a person who had acquired it
11 in unlawful ways may face remedies for the benefit of the original holder.

12 **Illustration:**

13 132. Before Directive (EU) 2016/943, trade secrets law in some European jurisdictions was
14 more or less pure tort law. Where H unlawfully stole one of C’s trade secrets and sold
15 it to T, who acted in good faith, only H would have been a tortfeasor, but not T. This
16 would not have been an effect ‘similar’ to IP protection. Since the implementation of
17 the Directive, trade secrets also take effect against third parties who had acquired the
18 trade secret in good faith from a person who had acquired it unlawfully, if the third
19 party later becomes aware of these facts. So trade secrets in the EU can now be
20 considered as affording their rightful holder a ‘similar’ right within the meaning of
21 Principle 29(1)(c).

22 *b. A general data ownership right?* There has been much discussion about whether there is
23 such a thing as ‘ownership’ in data, and if so, what it would mean. There can be little doubt that
24 information as such is not subject to ‘ownership’ but is normally free in the absence of specific
25 doctrines, such as trade secret law, that restrict rights with respect to it. Data, as the term is used in
26 these Principles, is different from information, in that it is information recorded on a medium and
27 typically expressed in code (such as a characteristic binary string of 0 and 1). Legal regimes have
28 recognized this difference in a number of ways, such as by giving greater rights to control access
29 to data than to control access to information. Whether data can constitute ‘property’ that can be
30 ‘owned’ is a topic that is subject of debate. After all, while data (or control of it) can have economic

1 value, data is a non-rivalrous resource that can be duplicated or multiplied at basically no cost,
2 making it different in important ways from traditional forms of property. These Principles take no
3 position as to whether data constitutes ‘property’ that can be ‘owned’, but if a legal system
4 introduced such an ownership right, and if it had third-party effects per se, it would be subsumed
5 under Principle 29(1)(c) or (a), depending on the nature of the right in the relevant legal system.

6 *c. Effects governed by the applicable law.* Principle 29(2) clarifies that, even though the
7 rights mentioned in Principle 29 have third-party effect per se, this holds true only for the ‘core
8 right’ as such, whereas the exact extent to which rights within the meaning of paragraph (1) limit
9 data activities, as well as the effect of such limitations, is determined by the applicable law. While
10 other *erga omnes* rights, such as ownership in tangible property or health and bodily integrity of a
11 natural person, normally enjoy quite comprehensive protection against all sorts of interference,
12 other *erga omnes* rights, including the rights listed in Principle 29, are normally more limited and
13 afford protection only against a defined range of activities.

14 **Illustration:**

15 133.C holds the copyright in large amounts of text data. P uses the copyright-protected
16 material, which is accessible online, intended for human readers, for training AI (so-
17 called text and data mining, TDM). Training the AI on the text does not automatically
18 interfere with C’s copyright, but only if training AI is generally among the activities
19 which the holder of copyright is entitled to control and where no exception from
20 copyright protection applies. Thus, the question whether the data activities pursued by
21 P are wrongful vis-à-vis C cannot be answered without an in-depth analysis of the
22 content and limits of copyright protection under the applicable law.

23 Given that the degree and form of protection varies from jurisdiction to jurisdiction, the
24 question whether or not a data activity is wrongful vis-à-vis the holder of a right within the
25 meaning of Principle 29 depends on which jurisdiction’s law applies in the individual case.

26 **REPORTERS’ NOTES:**

27 **U.S.**

28 The distinction between rights effective only between parties in privity with each other and
29 those that are effective against third parties is well known in the United States. In the law of secured
30 transactions, for example, the requirements for a security interest that is enforceable (*i.e.*, effective

1 only [with few exceptions] between the parties) and one that is perfected (effective against third
2 parties) differ. See UCC §§ 9-203 and 9-308. The distinction is recognized not only in the common
3 law states but also in Louisiana, which is a civil law state. See, e.g., the discussion of the distinction
4 in the context of assignment and subrogation in Saul Litvinoff, *The Law of Obligations* § 11.32, at
5 283 (Louisiana Civil Law Treatise, Vol. 5, 1992): “subrogation is effective against third persons,
6 including the obligor, from the time it takes place, which is expressed by saying that it produces
7 effects erga omnes, while an assignment of rights requires notice to the debtor or his express
8 acceptance in order to be effective against third persons.”

9 Europe:

10 *a. Traditional erga omnes rights. (i) Copyright.* Besides ownership, copyright is one of the
11 most important rights with third-party effects. European copyright law has been harmonized by the
12 Information Society Service Directive (Directive 2001/29/EC), which has recently been amended
13 by the Copyright DSM Directive (Directive (EU) 2019/790). In addition, the EU has adopted a
14 number of specific instruments in the field, such as the Database Directive (Directive 96/9/EC) and
15 the Software Directive (Directive 2009/24/EC). The European legal framework on copyright does
16 not provide for a list of types of protected works, as the Berne Convention does. In principle any
17 type of work can enjoy copyright protection as long as it meets the legal requirements that the work
18 is an expression of an idea that manifests itself in some material or concrete form and is ‘original’.
19 These requirements are explicitly stated in the Software Directive, which protects computer
20 programs by copyright as literary works. Excluded from the scope are ideas and principles which
21 underlie any element of a computer program (Article 1(2) Software Directive). The protection of a
22 ‘computer program’ requires that it is original in the sense that it is the author’s own intellectual
23 creation (Article 1(3) Software Directive). According to the still prevailing view, the ‘author’ must
24 be human, and a machine, even if powered by advanced AI, would not suffice. Data that is
25 measured by sensors or produced by machines could therefore only be covered where the design
26 of the data can directly be traced back to the software designer (Andreas Wiebe, *Protection of*
27 *industrial data – a new property right for the digital economy*, 2016 *Gewerblicher Rechtsschutz*
28 *und Urheberrecht International*, p. 877, 879). However, the European Parliament has recently
29 taken the view that technical creations generated by AI technology must be protected under IP law
30 in order to encourage investment and improve legal certainty for citizens, businesses and inventors
31 (European Parliament resolution of 20 October 2020 on intellectual property rights for the
32 development of artificial intelligence technologies (2020/2015(INI), P9_TA(2020)0277, No. 15).
33 The Parliament called on the Commission to support common, uniform copyright provisions
34 applicable to AI-generated works in the Union for cases where such works could be eligible for
35 copyright protection (*ibid*, No. 15).

36 The Database Directive establishes a legal framework for two types of intellectual property
37 rights relating to databases. First, the Directive clarifies in Article 3(1) that databases can qualify
38 for copyright protection if they satisfy the creativity and originality criterion that applies to any
39 other copyright protected work. Second, the Directive introduces a *sui generis* protection for
40 databases, if the maker ‘shows that there has been qualitatively and/or quantitatively a substantial
41 investment in either the obtaining, verification or presentation of the contents to prevent extraction
42 and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or
43 quantitatively, of the contents of that database’. However, the scope of the database protection is
44 very limited. According to the British Horseracing (Case C-203/02 ECLI:EU:E:2004:695 – *British*
45 *Horseracing*) and Fixtures Marketing (Case C-46/02 ECLI:EU:C:2004:694 – *Fixtures Marketing*)
46 judgments of the CJEU, the Directive does not protect investments in the creation of new data but

1 only the identification and collection of existing material. Therefore, investments in data creation
2 are excluded from the scope of the *sui generis* right. Due to this limitation in scope, data producers
3 will often fail to meet the requirements to qualify as creators of a database. However, especially
4 where data is generated by connected devices, the differentiation between the creation of new data
5 and the collection of existing data may not always be clear. In the *Autobahnmaut* case (Case I ZR
6 47/08 – *Autobahnmaut*), the German Supreme Court held that the private company Toll Collect
7 has a *sui generis* right in the dynamic database used for billing the individual operators. The
8 Supreme Court argued that the data registered by the terminals and vehicles was not ‘created’ by
9 Toll Collect but existed independently of the investment made by the database maker.

10 (ii) *Data privacy*. The protection of personal data is a fundamental right protected by the
11 Article 8 of the Charter of Fundamental Rights of the European Union. Furthermore, the GDPR
12 (Regulation (EU) 2016/679) provides for an extensive protection of personal data against any
13 infringements, including by third parties. The Regulation defines personal data broadly as ‘any
14 information relating to an identified or identifiable natural person (‘data subject’); an identifiable
15 natural person is one who can be identified, directly or indirectly, in particular by reference to an
16 identifier such as a name, an identification number, location data, an online identifier or to one or
17 more factors specific to the physical, physiological, genetic, mental, economic, cultural or social
18 identity of that natural person’ (Article 4(1) GDPR). This broad concept renders it rather difficult
19 for those responsible for anonymising personal data and thus escaping the protection regime of the
20 GDPR. The processing of personal data is only lawful if it is justified by one of the grounds listed
21 in Article 6, or, for more sensitive categories of data (such as health data), in Article 9.

22 The ePrivacy Directive (Directive 2002/58/EC) provides the basic legal framework for data
23 protection in electronic communications. Currently, a revision of the ePrivacy Directive is being
24 discussed at EU level (COM(2017), 10 final). Most recently, a Presidency discussion paper of the
25 Proposal was published (ST 9931 2020 INIT). However, due to the many points of contention that
26 have remained unsolved so far, it is highly uncertain whether a new Regulation will finally be
27 adopted and what will be the policy choices made.

28 (iii) *Trade secrets*. Third-party effects may also arise from the Trade Secrets Directive. A
29 trade secret is defined as information that meets the following requirements: (a) it is secret in the
30 sense that it is not, as a body or in the precise configuration and assembly of its components,
31 generally known among or readily accessible to persons within the circles that normally deal with
32 the kind of information in question; (b) it has commercial value because it is secret; and (c) it has
33 been subject to reasonable steps under the circumstances, by the person lawfully in control of the
34 information, to keep it secret. The definition of a trade secret is almost identical to that of the
35 protection of undisclosed information in Article 39 of the Agreement on Trade-Related Aspects of
36 Intellectual Property Rights (TRIPS). According to Article 39(2), natural and legal persons shall
37 have the possibility of preventing information lawfully within their control from being disclosed
38 to, acquired by, or used by others without their consent in a manner contrary to honest commercial
39 practices so long as such information: (a) is secret in the sense that it is not, as a body or in the
40 precise configuration and assembly of its components, generally known among or readily
41 accessible to persons within the circles that normally deal with the kind of information in question;
42 (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under
43 the circumstances, by the person lawfully in control of the information, to keep it secret. However,
44 the Trade Secrets Directive does not grant an exclusive right to data as such, since the protection
45 under the Directive depends on the factual existence of a secret and is thus more similar to the
46 protection of possession. Furthermore, the trade secret is not protected against any kind of use, but
47 only against certain forms of infringement under Article 4 of the Directive (see Herbert Zech,

1 ‘Information as a tradable commodity’, in: De Franceschi (ed.), European Contract Law and the
2 Digital Single Market, 2016, p. 51, 63 f.).

3 *b. A general data ownership right?* Finally, there has been a lively debate about ‘data
4 ownership’ in Europe. The debate may originally have been sparked in Germany, fueled by the
5 automobile and other industries worrying about the protection of IoT data they accumulate and by
6 the consumers’ desire to participate more in the profits made by the data economy. After the
7 European Commission mentioned the option of introducing a ‘data producer’s right’ at EU level
8 in its Communication on ‘Building a European Data Economy’ (COM(2017) 9 final, p. 10 ff.), the
9 debate spread throughout Europe. It soon became more or less common opinion, however, that the
10 concept of exclusive ownership rights in data that might be comparable to ownership in tangible
11 property or to intellectual property rights is not a good way forward. (see Opinion of the Data
12 Ethics Commission, 2019, p. 104 f.). It is commonly held that such a regime would have the
13 potential of suffocating the European data economy rather than boosting it, and given that
14 consumers would readily contract away their ownership, very much as they are currently
15 contracting away any other rights they have with regard to data, this is not likely to enhance
16 consumer rights either (Maartje Elshout et al., Study for the European Commission on consumer’s
17 attitudes towards terms and conditions, 2016, p. 9; Jonathan A. Obar and Anne Oeldorf-Hrisch,
18 The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of
19 Social Networking Services, (2018) 22 iCS 1). The predominant view in Europe currently is that
20 access rights and similar data rights are the more promising way forward (COM(2020) 66 final, p.
21 4 ff.; COM(2018) 232 final, p. 9; see also Reporters’ Notes to Principle 23).

22 **Principle 30: Contractual limitations**

23 **(1) For the purpose of Principle 28(1)(b), a contractual limitation on data activities is a**
24 **contractual term that limits data activities of any party to the contract, including by**
25 **limiting the use or onward transfer of data.**

26 **(2) In determining whether a contractual limitation on data activities is in conflict with**
27 **mandatory rules of law that vindicate important public policies and those that protect**
28 **parties from overreaching conduct or agreements, factors to be taken into account**
29 **include whether the agreement**

30 **(a) unduly limits the freedoms of a contracting party, taking into account, inter alia,**
31 **comparable limits of intellectual property protection;**

32 **(b) unduly limits activities in the public interest; or**

33 **(c) has unjustified discriminatory or anti-competitive effects.**

34 **Comment:** *a. Contractual protection as compared with IP protection.* According to
35 Principle 28(1)(b), data activities are wrongful if they fail to comply with contractual limitations

1 within the meaning of Principle 30. In practice, contractual limitations, such as in data transactions
2 of the type described in Part II, are common and used to substitute for the often-missing protection
3 provided by intellectual property law. However, contractual protection works in a somewhat
4 different manner.

5 Intellectual property rights create an exclusive right, to the extent provided under
6 intellectual property law, on the part of the rightholder to exploit the economic potential of a
7 particular intellectual achievement, either by using it directly or by licensing it to others. The same
8 holds true, in principle, for IP-like schemes of investment protection. As far as IP protection is
9 afforded by the law, no third party may use the same intellectual achievement except with the
10 rightholder's permission under a license. A license may be granted under conditions, but there are
11 limits, notably limits posed by the exhaustion principle (first sale doctrine), and there are certain
12 types of fair use, whether or not exhaustively listed in statutes, that are typically open to every third
13 party.

14 Where data is not protected by IP law or any similar scheme, as is the case with many
15 collections of data that are neither computer programs nor literary works nor otherwise protected
16 by copyright or a related right, this does not automatically mean that the controller must keep the
17 data absolutely closed down and secret if it does not want the data to be freely available to everyone.
18 Rather, where a party is in control of data, and is not under an obligation to share the data with
19 others, this person can make an offer to particular other parties or to the public at large to use the
20 data on the basis of particular terms that are essentially contractual in nature. Generally speaking
21 and subject to contract and other doctrines that protect the public interest and contractual
22 protections against overreaching and oppressive terms, those terms will be enforced.

23 **Illustration:**

24 134. Business Y operates a website on which customers can search through flight data of
25 various airlines, compare prices and, on payment of a commission, book a flight. Y
26 obtains the necessary data to respond to an individual query by automated means, inter
27 alia, from a dataset linked to the publicly accessible website of airline X. Access to that
28 website presupposes that the visitor to the site effectively accepts the application of X's
29 general terms and conditions by ticking a box to that effect. The terms include a clause
30 reading 'The use of automated systems or software to extract data from this website for
31 commercial purposes is prohibited unless the third party has directly concluded a

1 written license agreement with X.’ If Y ticks the box by automated means and uses X’s
2 website in breach of the terms, Y has breached its agreement with X and thus Y’s data
3 activities are wrongful under Principles 28(1)(b) and 30.

4 *b. Limits of protection as between the contracting parties.* Principle 30 does not address
5 what is required to make a valid contract, or to effectively impose a contractual limitation on the
6 other party. As to the first point of contract formation, this may, in practice, be particularly difficult
7 to establish in cases of data harvesting (data scraping) where the data collected is, in principle,
8 publicly accessible on websites. The difficulties are largely related with establishing meaningful
9 assent, and the situation could be considered to be similar to the provision of unsolicited services.

10 Formation of contract apart, general contract law, or special categories of contract law (such
11 as consumer contract law), are also relevant as far as the substantive validity of terms is concerned.
12 For instance, terms may be held to be objectionable, such as under doctrines of unconscionability
13 or unfairness (where applicable), and there may be concerns under other doctrines related to public
14 policy. As such doctrines diverge across different legal systems, paragraph (2) provides some
15 guidance as to the circumstances the law ought to consider in determining whether terms are
16 objectionable. In particular, paragraph (2) mentions consideration of whether the agreement unduly
17 limits the freedoms of a contracting party limits activities in the public interest, and whether those
18 limitations have unjustified discriminatory or anti-competitive effects

19 **Illustration:**

20 135. Assume that, in Illustration no. 134, the clause used by airline X reads ‘Extraction of
21 data from this website for the purpose of comparing our prices with prices of other
22 airlines is prohibited.’ This clause might, depending on the context, be held to be
23 objectionable because of its anti-competitive effects.

24 It is a matter of some controversy whether fair use, first sale doctrine and similar limiting
25 concepts limit only intellectual property rights or if they also limit the reach of contractual terms
26 that might provide for additional restrictions beyond those imposed by intellectual property law or
27 limit the reach of contractual restrictions imposed on data not protected by intellectual property
28 law. These Principles are generally favorable to the view that contractual limitations should
29 normally not go further than would be permitted by comparable IP law regimes, but there should
30 be some flexibility to allow for the consideration of all elements of the case.

1 for tortious interference with hiQ’s contracts with third parties when LinkedIn sought to prevent
2 hiQ’s bots from downloading public, non-proprietary data from LinkedIn’s website.

3 With respect to the possibility of extending exclusive rights by contract when they are no
4 longer available through intellectual property law, see, *e.g.*, *Impression Products, Inc. v. Lexmark*
5 *Intern., Inc.*, 137 S.Ct. 1523 (2017). See also Nancy S. Kim, *Revisiting the License v. Sale*
6 *Conundrum*, 54 Loy. L.A. L. Rev. 99 (2020).

7 With respect to unconscionability, see generally UCC § 2-302 and Restatement (Second),
8 Contracts, § 208 and cases decided thereunder.

9 With respect to contracts that violate public policy, see Restatement (Second), Contracts §§
10 178-79 (particularly § 178(2)-(3), providing factors supporting enforcement and opposing
11 enforcement).

12 With respect to contracts that have an anti-competitive effect, see Restatement (Second),
13 Contracts §§ 186-88.

14 More generally, see NANCY S. KIM, *CONSENTABILITY: CONSENT AND ITS LIMITS* (2019);
15 NANCY S. KIM, *WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS* (2013); Mark Lemley,
16 *Terms of Use*, 91 MINN. L. REV. 459 (2006).

17 **Europe:**

18 *a. Contractual protection as compared with IP protection.* Rights arising out of contracts
19 can generally only be asserted against the contractual partner. Only in a limited range of situations
20 are they also protected against interference by third parties (see Reporters’ Notes to Principle 34).
21 While one may assume that rights with third-party effect offer higher protection than contractual
22 rights, this may not necessarily be the case, as rights with third-party effect do not only afford
23 protection but may also limit party autonomy. Therefore, the absence of rights with third-party
24 effects can be an advantage for the controller, if – based on the contractual freedom of the parties
25 – they agreed upon a more extensive and specific protection (see Benoit Van Asbroeck, Julien
26 Debussche and Jasmien César, *Building the Data Economy – Data Ownership – Whitepaper*
27 (2017), p. 99). The CJEU’s *Ryanair* case (Case C-30/14 ECLI:EU:C:2015:10 – *Ryanair Ltd*) is a
28 prime example of how the absence of a right with third-party effect may lead to greater protection.
29 In this case the CJEU considered that the provisions on database copyright and the *sui generis*
30 right, which limit contractual freedom, do not apply to the database in question. Consequently, the
31 author/producer of such a database is free – subject to compliance with the applicable national law
32 – to determine the contractual provisions governing the use of the database, which may lead to an
33 even higher level of protection than under the provisions of the database copyright and the *sui*
34 *generis* right.

35 *b. Limits of protection between contracting parties.* European legal systems usually deal
36 with contractual restrictions on resale in the context of the acquisition of ownership. In the
37 Germanic legal traditions, it is generally assumed that contractual restrictions do not have any third-
38 party effect. Section 137 of the German Civil Code, for example, states that limitations on resale
39 are void with regard to the acquisition of ownership of the second purchaser. However, the
40 contractual promise not to resell has effect *inter partes*, and the party in breach may be liable. The
41 German provision is quite similar to Section 364c of the Austrian Civil Code, according to which
42 limitations on resale do not produce any third-party effect, but the validity of the agreement itself is
43 unaffected. The French Civil Code takes a somewhat different approach. Its Article 900-1 provides
44 that such clauses are valid under the conditions that the limitation is temporary and justified by a
45 serious and legitimate interest. Such a limitation of the transferability of an asset renders void any

1 subsequent transfer within the specified period (Cass. 3e civ., 31 mai 2006, n 8 05-10270), unless
2 the rules of good faith (Article 2276) apply.

3 The situation is different when it comes to copyright protected works. The resale of
4 computer programs cannot be prohibited, because once the computer program is sold, the
5 distribution right of that copy is exhausted, with the exception of the right to control further rental
6 of the program or a copy thereof (Article 4(2) of Directive 2009/24/EC). To what extent the
7 exhaustion principle also applies to digital content other than computer programs is still disputed,
8 but in a recent judgement the CJEU did not extend the first sale doctrine to E-Books (Case C-
9 263/18 ECLI:EU:C:2019:1111 –*Tom Kabinet*). In the *UsedSoft* decision, the CJEU defined ‘sale’
10 as an agreement by which a person, in return for payment, transfers to another person the right to
11 use the copy for an unlimited period (Case C-128/11 ECLI:EU:C:2012:407, para 42 ff – *UsedSoft*).
12 The distinction between use for an unlimited period and for a limited period is thus decisive for
13 whether a restriction on resale is effective. If the buyer is entitled to use the copy for an unlimited
14 period of time, restrictions only have third-party effects in exceptional cases, e.g. agreements that
15 prohibit further rental of the copyright protected work (see Article 4(2) of Directive 2009/24/EC).
16 However, if the recipient is only entitled to use the copy for a limited period of time, restrictions
17 on resale do have third-party effect. Under the copyright law of some European Member States,
18 the limitation on certain types of use may produce third-party effects, if the type of use is common,
19 technically and economically independent and thus clearly delimitable (e.g. use of a musical work
20 for advertising purposes, German Supreme Court I ZR 226/06; see also German Supreme Court I
21 ZR 244/97 – *OEM*).

22 Finally, there has been a lively discussion as to whether restrictions on use or resale can (at
23 least) take effect against the contractual party when they are included in terms and conditions. The
24 main argument against the validity of such agreements is that the principle of exhaustion is based
25 on considerations of fairness. The Unfair Contract Terms Directive (UCTD, Council Directive
26 93/13/EEC) considers contractual terms in consumer contracts as unfair and not binding if they are
27 not individually negotiated and cause, contrary to the requirement of good faith, a significant
28 imbalance between the parties’ rights and obligations, to the detriment of the consumer (Article
29 3(1)). In several Members States unfairness control of standard clauses is not applied only to
30 consumer contracts but, at least in principle, extended to B2B relationships. However, with regard
31 to user accounts and computer games, the German Supreme Court decided in the famous *Half Life*
32 2 decision that even if it is possible to resell a computer game because the right is exhausted, it is
33 still possible to validly restrict the resale of the user account in the terms and conditions (German
34 Supreme Court, Case I ZR 178/08 – *Half Life 2*). Nevertheless, the currently dominant view is –
35 especially after the *UsedSoft* decision of the CJEU – that terms and conditions that are not in line
36 with copyright law are unfair and therefore void under the UCTD. This is mainly based on the
37 argument that the principle of exhaustion also aims to achieve a fair balance between the interests
38 of the parties involved, just as the statutory default regimes do.

39 Principle 31: Unauthorized access

40 **(1) For the purpose of Principle 28(1)(c), access to data has been obtained by unauthorized**
41 **means if it has been obtained by:**

42 **(a) circumvention of security measures;**

1 **(b) taking advantage of an obvious mistake, such as security gaps that the person**
2 **accessing the data could not reasonably believe the controller had intended; or**

3 **(c) interception by technical means of non-public transmissions of data, including**
4 **electromagnetic emissions from a medium carrying data.**

5 **(2) Access to data has not been obtained by unauthorized means if**

6 **(a) access to the data is allowed under an agreement between the person accessing the**
7 **data and the controller; or**

8 **(b) the person accessing the data had a right that, under other law (such as law relating**
9 **to freedom of information and expression), prevails over the controller's right under**
10 **this Principle.**

11 **Comment:** *a. General observations.* There are situations where data activities do not
12 infringe a right with third-party effect under Principle 29, or contractual limitations under Principle
13 30, but where the activities (and, in fact, the mere access to or control of data itself) should
14 nevertheless be considered wrongful. This is the case where a person pursuing data activities has
15 obtained access to the data in a way that is manifestly dishonest and, amongst others, disapproved
16 by international law such as the Budapest Convention on Cybercrime.

17 **Illustration:**

18 137. Where P has raw machine data stored in password-protected cloud space provided by
19 cloud provider C, and Y hacks the cloud space and clandestinely uses the data, Y's
20 control is wrongful even though P does not own the medium and the data was neither
21 protected by intellectual property law nor a trade secret. The same should apply where
22 Y does not hack the cloud space but clandestinely intercepts the machine data during
23 transmission to the cloud.

24 Apart from the situation where a person intentionally infringes security measures or
25 clandestinely intercepts data, the law should also intervene where a person intentionally exploits
26 an obvious mistake by the controller. One form of such obvious mistakes are security gaps which
27 that person could not reasonably have believed the controller had intended. The same should hold
28 true when access credentials have been accidentally supplied to the wrong recipient and this was
29 obvious to the recipient.

1 **Illustration:**

2 138. Where, in Illustration no. 137, C's password protection scheme is down for a few hours
3 and Y takes advantage of the situation and obtains access to P's data, this should be
4 treated in the same manner as if Y had hacked the cloud space, because Y could not
5 reasonably have believed that C had deliberately switched off protection.

6 Principle 31(1)(b) should apply all the more where the mistake was induced by the person
7 obtaining unauthorized access, such as by way of deceit (e.g. phishing). On the other hand, access
8 obtained by mere non-compliance with contractual prohibitions, or with prohibitions unilaterally
9 declared by the controller, is insufficient to make access unauthorized within the meaning of
10 Principle 31.

11 **Illustration:**

12 139. Z uses a webcrawler for harvesting data that happens to be publicly available in social
13 media. In order for the webcrawler to access the social network provided by provider
14 P, the terms and conditions need to be accepted by ticking a box, which Z (or its
15 webcrawler) does. In P's terms and conditions, such 'spidering' activities are explicitly
16 prohibited. This might amount to a data activity that is wrongful under Principle 30, but
17 not to unauthorized access within the meaning of Principle 31.

18 *b. Authorization.* Paragraph (2) clarifies that access to or operations on data by a person are
19 not unauthorized where authorization follows from a valid agreement between the person and the
20 controller, or the person had a right under other law that prevails over the controller's right.

21 **Illustration:**

22 140. Employee E of company C terminates her employment contract with C and leaves the
23 company, without handing over the access credentials to her workplace computer on
24 which important company files are stored, despite a clause in the employment contract
25 and a reminder by C. C finally gets access to the files with the help of an IT specialist,
26 basically hacking E's account. C has not acted in an unauthorized manner because
27 access to the files was authorized by the employment contract.

1 [Note to the American Law Institute: Comment *b* and this Illustration will be revisited by
2 the Reporters after the decision of the Supreme Court of the United States in *United States v. Van*
3 *Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (argued November
4 30, 2020).]

5 **REPORTERS' NOTES:**

6 **U.S.:**

7 The U.S. Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, imposes criminal
8 and civil liability on those who knowingly or intentionally access a variety of data without
9 authorization. The broadest category is access without authorization or exceeding authorization to
10 information on a protected computer, defined to be computers used exclusively by financial
11 institutions or computers used in or affecting interstate or foreign commerce or communication,
12 including computers located outside the U.S. Courts have held that evasions of IP blocks and access
13 by former employees after their authorization has been revoked constitute CFAA violations.
14 *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016); *United States v. Nosal*, 844
15 F.3d 1024, 1035-37 (9th Cir. 2016); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 962 (N.D. Cal.
16 2013). The Supreme Court is currently considering whether persons who are authorized to access
17 information for certain purposes but access that information for an improper purpose violate the
18 CFAA. *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667
19 (2020). Questions remain about the scope of CFAA liability for those conducting research.
20 *Compare, e.g., United States v. Auernheimer*, No. 2:11-470-01, 2013 WL 1774234 (D.N.J. Mar.
21 19, 2013) (convicting defendant under the CFAA for program analyzing security flaw), *vacated*
22 *for improper venue*, 748 F.3d 525 (3d Cir. 2014), *with Sandvig v. Barr*, 451 F. Supp. 3d 73 (D.D.C.
23 2020) (holding violation of terms of service insufficient constitute a criminal violation of the
24 CFAA).

25 With respect to copyrighted material, the Digital Millennium Copyright Act prohibits the
26 circumvention of technical measures that control access to copyrighted works or manufacturing,
27 providing or otherwise trafficking in any technology or product capable of circumventing such
28 technical measures. 17 U.S.C. § 1201(a)-(b).

29 All fifty U.S. states have enacted statutes prohibiting unauthorized access to computer
30 systems. Computer Crime Statutes, Nat’l Conf. of State Legis. (Feb.. 24, 2020),
31 [https://www.ncsl.org/research/telecommunications-and-information-technology/computer-](https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx)
32 [hacking-and-unauthorized-access-laws.aspx](https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx).

33 **Europe:**

34 *a. General observations.* The Budapest Convention on Cybercrime (Council of Europe
35 Treaty No. 185, 23 November 2001) prohibits any intentional access to the whole or any part of a
36 computer system ‘without right’, which infringes security measures. A similar protection against
37 the circumvention of ‘effective technological measures’ can be found in the Information Society
38 Service Directive (Directive 2001/29/EC). ‘Technological measures’ is defined as any technology,
39 device or component that, in the normal course of its operation, is designed to prevent or restrict
40 acts, in respect of works or other subject matter. The acquisition of a trade secret is considered
41 unlawful under the Trade Secrets Directive (Directive (EU) 2016/943) if carried out by
42 unauthorized access to documents, objects, materials, substances or electronic files that are

1 lawfully under the control of the trade secret holder and which contain the trade secret or from
2 which the trade secret can be deduced (Article 4(2)(a)).

3 Unauthorized access to rival goods constitutes a violation of the right of possession and
4 may be subject to possessory remedies as well as to liability claims under tort law or claims of
5 unjust enrichment. In European legal systems, possessory remedies are usually available if
6 interference with possession occurs without the possessor's consent or a legal ground (see Article
7 VIII. – 6:201 Principles of European Law, Acquisition and Loss of Ownership in Good; Section
8 339 of the Austrian Civil Code; Section 858 of the German Civil Code).

9 *b. Authorization.* Grounds on the basis of which interference can be justified by law are,
10 *inter alia*, statutory rights to withhold or rights of self-help. A person is typically entitled to
11 withhold physical control over a good until compensated for labour or financial expenditure for the
12 benefit of the property. The right to self-help is usually subject to very restrictive conditions.
13 Certain jurisdictions require that help by the competent state authorities would come too late (see
14 Section 344 Austrian Civil Code). Other jurisdictions require that the self-help reaction complies
15 with a certain standard of necessity and that it is reasonable and proportionate to the damage
16 inflicted. Furthermore, self-help is permitted only within strict time limits. Besides private law,
17 interference can also be justified by public law, such as judicial enforcement proceedings.

18 Chapter B: Effects of Onward Supply on the Protection of Others

19 Principle 32: Duties of a supplier in the context of onward supply

20 **(1) Where a party supplying data to a recipient may pass the data on but is obligated to**
21 **comply with duties and restrictions within the meaning of Chapter A, the law should**
22 **require the supplier to**

23 **(a) impose the same duties and restrictions on the recipient (unless the recipient is**
24 **already bound by them), including the duty to do the same if the recipient supplies**
25 **the data to other parties; and**

26 **(b) take reasonable and appropriate steps (including technical safeguards) to assure**
27 **that the recipient, and any parties to whom the recipient may supply the data, will**
28 **comply with those restrictions.**

29 **(2) Where the supplier later obtains knowledge of facts that indicate wrongful data**
30 **activities within the meaning of Principle 28 on the part of a recipient, or that render**
31 **data activities by the recipient wrongful or would otherwise require steps to be taken**
32 **for the benefit of a protected party, the supplier must take reasonable and appropriate**

1 **measures to stop wrongful activities or to take such other steps as are appropriate for**
2 **the benefit of a protected party.**

3 **(3) Nothing in this Principle precludes strict vicarious liability of a controller for data**
4 **activities by a processor under the applicable law.**

5 **(4) Whether the supplier’s duties under this Principle may be waived by the protected party**
6 **or varied by agreement to the detriment of that party is determined by the nature of the**
7 **relevant duties and restrictions under Chapter A and any applicable rules of law that**
8 **make those duties non-waivable by the protected party.**

9 **Comment:** *a. General observations.* Where data is passed on from one controller to
10 another, this always poses a challenge for the protection of others within the meaning of Chapter
11 A. On the one hand, risks of infringement multiply with any increase in the number of controllers
12 ultimately holding the data. The more controllers there are, the more difficult they are to identify,
13 and it may become next to impossible for a protected party within the meaning of Chapter A to
14 enforce its rights. On the other hand, most data existing worldwide is probably, at least potentially,
15 subject to some restriction of data activities following from Chapter A. Anyone receiving receiving
16 data from multiple sources may be confronted with a multitude of protection requirements, some
17 of them difficult to recognize, and some of them for the remote protection of parties that are
18 connected only through a long chain of transactions. This may have a serious chilling effect on data
19 activities. These Principles thus need to strike a balance between third party protection and the
20 protection of data recipients.

21 Chapter B deals with the effects that onward supply of data has on the protection of other
22 parties within the meaning of Chapter A, and the effects of such protection on the onward supply.
23 Onward ‘supply’ of data is to be understood broadly and is not restricted to contracts for the supply
24 of data within the meaning of Part II, Chapter B. In particular, it includes any provision of access
25 to the data to a processor or other service provider under Part II, Chapter C. Onward supply does
26 not require any contract between the supplier and the recipient, in particular not where data is
27 supplied in order to comply with an access right within the meaning of Part III. Principles 20(3)
28 and 25(a) explicitly clarify that the duties of a supplier apply to controllers that must comply with
29 data rights. Principles 20(2) and 24(3) ensure that data rights are afforded only with such

1 restrictions as enable the controller to comply with both the data right and the duties under Principle
2 32.

3 *b. Direct effect vs due diligence duties vs strict vicarious liability.* There are essentially
4 three ways in which the law can make the difficult balance between third-party protection and the
5 protection of data recipients.

6 The first possible mechanism is that of direct effect, i.e. a protected third party is afforded
7 the same rights (and possibly remedies) against a downstream recipient as the protected third party
8 had against the previous link in the chain of transactions. This mechanism may be part of a wider
9 framework (see Principle 33), but it certainly cannot be the only solution, as it would both burden
10 protected parties with enforcing their rights against a series or even a multitude of different
11 controllers, whose identity may not even be known to them, and burden the recipients with a
12 potential multitude of claims from parties they are not aware of.

13 The second possible mechanism is that of due diligence duties for suppliers, i.e. anyone
14 who (rightfully) supplies data to another party must make sure that it chooses only recipients that
15 will comply with the same restrictions the supplier had to comply with, and has to take further steps
16 to safeguard the interests of protected parties, including technical and institutional safeguards.
17 Under this mechanism, which is reflected in Principle 32, the supplier is liable only for breach of
18 its own due diligence duties, i.e. where a supplier can demonstrate that it has done everything that
19 could be expected from it, and, despite all safeguards, a downstream supplier engages in wrongful
20 data activities, the supplier would not be liable to a protected third party for the activities of the
21 downstream recipient.

22 The third possible mechanism is that of strict vicarious liability. Under this mechanism, the
23 law remains largely silent as to the duties of a supplier when passing on data, but whoever passes
24 on data does so at its own risk and will be strictly liable for whatever happens in terms of wrongful
25 data activities downstream. On the one hand, this is efficient, as it leaves the decision as to the
26 appropriate safeguards to the supplier and lowers overall costs of compliance. On the other hand,
27 liability risks may become incalculable where the recipient again passes the data on, assuming that
28 the first supplier is also liable for any wrongful activities far down the chain of transactions (if a
29 law opted for this model but failed to provide for liability of the supplier for activities further down
30 the chain of transactions this might lead to massive undercompensation of protected parties
31 suffering harm). Also, the supplier is not always the stronger party, but may be a small retailer

1 passing data on to a multinational company and without much of a choice, which would make it
2 seem inequitable to hold that retailer strictly liable for anything wrongful happening downstream.
3 This is why, ultimately, these Principles do not propose strict vicarious liability as the general rule.
4 However, strict vicarious liability may be justified where data is entrusted to a service provider
5 within the meaning of Part II, Chapter C, see paragraph (3).

6 *c. Duty to pass on restrictions.* Principle 32(1)(a) provides in the first place that, even where
7 onward supply of data as such is rightful, the supplier of data is under a duty to pass on to the
8 recipient all the duties and restrictions which the supplier itself had to comply with for the benefit
9 of a protected party within the meaning of Chapter A, unless the recipient is already bound by those
10 duties and restrictions. This includes the duty to impose the same duties and restrictions on any
11 downstream recipient to which the recipient may, in turn, make the data available. In most cases,
12 protected parties will be either holders of intellectual property rights with regard to the data or data
13 subjects protected under data privacy/data protection law (i.e. parties protected under Principle 29)
14 or upstream suppliers that had imposed on the supplier particular contractual limitations under
15 Principle 30. In some cases, such as where protected parties are holders of intellectual property
16 rights, recipients would likely be already bound by the restrictions imposed by the intellectual
17 property regime in any case.

18 Where the duty or restriction already follows from the law, all that is normally required by
19 Principle 32(1)(a), without prejudice to more far-reaching duties under Principle 32(1)(b), is that
20 the supplier chooses trustworthy recipients, i.e. applies due diligence in assessing whether the
21 recipient will most likely act in a compliant manner, and, where necessary, informs these recipients
22 of the existence of the relevant rights on the part of protected parties. However, where the duty or
23 restriction would normally bind only the supplier, such as a contractual duty or restriction, the
24 supplier may not supply the data to a recipient that does not agree to comply with the same duties
25 or restrictions. If the supplier still passes the data on, this data activity would be considered
26 wrongful under these Principles and, if the requirements of Principle 34 are met, also the data
27 activities of the recipient.

28 **Illustration:**

29 141. Supplier S of bulk data agrees with the first recipient R1 that R1 may use the data for
30 all lawful purposes except a defined list of purposes that would harm S's economic

1 interests. If R1 supplies the data to R2 (provided this is not excluded under the contract
2 with S), R1 is under an obligation to impose the same restrictions with regard to data
3 use on R2, i.e., under the contract with R1, R2 also must agree not to process the data
4 for the defined list of purposes that would harm S's economic interests.

5 In particular where due diligence leads to the assessment that the recipient might not
6 effectively comply with the duties and restrictions imposed the supplier must, under Principle
7 32(1)(b), adopt additional safeguards that provide an appropriate level of certainty, or refrain from
8 making the data available to the recipient. Such additional safeguards can be of a legal nature, such
9 as prohibitively high penalties (where allowed) in cases of non-compliant activities, or of a
10 technical nature, such as technical means that ensure that non-compliant activities are prevented.
11 They may also include institutional arrangements such as using the services of a data trustee or
12 data escrowee within the meaning of Principles 13 and 14.

13 These Principles do not define exactly which steps can be expected in which kind of
14 situation. Generally speaking, a risk-based approach must be taken, i.e. the more 'sensitive' the
15 data and the greater the potential risks for protected third parties that may follow from non-
16 compliant data activities, the stricter and more effective the safeguards that the supplier must
17 ultimately take. The steps that can reasonably be expected from a supplier also depend on the
18 relationship between the supplier and the recipient. Where the recipient is a processor that
19 processes the data on the supplier's behalf, the supplier normally has greater influence on the
20 recipient and on how the recipient deals with the data (but this is not necessarily the case, e.g. when
21 a small business uses the services of a big processor, such as a big cloud space provider).

22 *d. Duty to monitor and remediate wrongful activities.* Paragraph (2) stresses that, where the
23 supplier later obtains knowledge of facts that indicate wrongful processing on the part of the
24 recipient, render data activities by the recipient wrongful, or would otherwise require steps to be
25 taken for the benefit of a protected party, the supplier must take reasonable and appropriate steps
26 to stop wrongful activities, and protect the protected party. The reason why paragraph (2) requires
27 knowledge (and not merely 'notice') is that a controller can normally not be expected to
28 continuously monitor and call into question any kind of onward supply that occurred in the past.
29 This normally means that the supplier must inform the recipient where the recipient may be
30 unaware of the wrongfulness. The technical and other arrangements must be such as to ensure that

1 the information reaches the recipient as early as the circumstances require, in particular where the
2 recipient is a processor.

3 **Illustration:**

4 142. Business S operates a video game and supplies personal user data to recipient R, which
5 is lawful under the applicable European data protection regime because users have
6 given consent. Where S learns of the withdrawal of consent by some of its users further
7 control by both S and R of this personal user data will usually become wrongful, and
8 they will usually be under an obligation to erase this data. S must pass this information
9 on to R in order to direct R to erase the data. If R is not a controller, but a processor
10 processing data on behalf of S, S must take even more rigorous action and immediately
11 stop processing by R of the data of the users who have withdrawn consent.

12 However, Principle 32(2) only requires steps that are reasonable and appropriate, again
13 taking a risk-based approach and considering the relationship between the supplier and the
14 recipient, including the degree of influence which the supplier has on the recipient.

15 **Illustration:**

16 143. W runs a website with a large quantity of information that can be downloaded freely.
17 W then learns that one of the documents offered for download was infringing X's
18 copyright, and therefore W immediately takes it off the website. W is aware that the
19 document has been downloaded 300 times, but W has no reasonable means of finding
20 out who these individuals are and how to contact them. In this situation, there is no
21 obligation to inform those individuals or take further action under this Principle.

22 *e. Waiver of duties.* Whether the supplier's duties under this Principle may be waived by
23 the protected (third) party or varied by agreement to the detriment of that party is determined by
24 the nature of the relevant duties and restrictions under Chapter A. If, for instance, the restriction
25 stems from a mandatory statutory regime such as data privacy/data protection law, any waiver by
26 the protected party, if it is at all possible, must occur within the boundaries set by that statutory
27 regime, which will be rather narrow. If the restriction stems from a contract between the protected
28 party and the supplier, the protected party can waive protection within the much broader limits set

1 by the applicable contract law, which may differ from jurisdiction to jurisdiction, and from scenario
2 to scenario (e.g. depending on whether the transaction is a B2C or B2B transaction).

3 **REPORTERS' NOTES:**

4 **U.S.:**

5 Contractual provisions embodying the duty to pass on restrictions are quite common in the
6 U.S.. See, e.g., the following language that appears in Law Insider, Sublicense Requirements
7 Sample Clauses, available at <https://www.lawinsider.com/clause/sublicense-requirements>: “Each
8 sublicense granted by a Party to a Third Party pursuant to Sections 2.1(b) or 2.2(b) (a “Sublicense”)
9 shall (a) be in writing; (b) be subject and subordinate to, and consistent with, the terms and
10 conditions of this Agreement; and (c) require the applicable sublicensee (the “Sublicensee”) to
11 comply with all applicable terms of this Agreement. [emphasis added].

12 Similarly, it is quite common for data license contracts to impose on a licensee a duty to
13 monitor the compliance with license terms by the sublicensee. See Daniel Glazer, Henry Lebowitz,
14 and Jason Greenberg, Data as IP and Data License Agreements (available at
15 [https://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20Licens
16 e%20Agreements%20\(1\).pdf](https://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20License%20Agreements%20(1).pdf)): a sublicense agreement should expressly specify “appropriate
17 sublicensing obligations (for example, the sublicensor’s responsibility for the actions of its
18 sublicensees ...”).

19 Some federal statutes require suppliers of data to impose legal duties on recipients. For
20 example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires
21 covered entities wishing to disclose protected health information to “business associates” to obtain
22 satisfactory assurances that the business associates will use the information only for the purposes
23 for which it was engaged by the covered entity, will safeguard the information from misuse, and
24 will help the covered entity comply with some of the covered entity’s duties under the Privacy
25 Rule.
26

27 **Europe:**

28 *c. Duty to pass on restrictions.* Duties to pass on restrictions can be found in the Standard
29 Contractual Clauses (SCC) for the transfer of personal data between European Union
30 (EU)/European Economic Area (EEA) and non-EU/EEA countries. Where an exporting controller
31 and an importing controller or processor include the SCC in their contract, the transfer of the data
32 outside the EU/EEA is considered to be in accordance with EU data protection legislation.
33 However, according to a recent judgment of the CJEU (C-311/18 ECLI:EU:C:2020:559 – *Schrems*
34 *II*) further steps may be required, such as establishment of a data escrow. Similar to Principle 33,
35 the terms of SCCs differ depending on whether the importing recipient is a controller or processor
36 (Commission Implementing Decision (EU) 2021/914).

37 The SCC have the purpose to ensure compliance with the requirements of the GDPR
38 (Clause 1(a)). The exporter, i.e. the supplier, warrants, that it has used reasonable efforts to
39 determine that the data importer, i.e. the recipient, is able, through the implementation of
40 appropriate technical and organisational measures, to satisfy its obligations under these Clauses
41 (Clause 8). If the importer is unable to comply with the SCC for whatever reason, it shall promptly
42 inform the data exporter (Clause 16(a)). The exporter shall be entitled to terminate the contract,
43 e.g., if the importer is in substantial breach or persistent breach of the SCC.

1 If the importer is a controller, the SCC provide for several obligations on data protection
2 safeguards. The importer shall, *inter alia*, not disclose the data to at third party located outside the
3 EU unless the third party is or agrees to be bound by the SCC. Moreover, the importer shall deal
4 with any enquiries and requests it receives from a data subject relating to the processing of his/her
5 personal data and the exercise of his/her rights under the SCC without undue delay and at least
6 within one month of the receipt of the enquiry.

7 Different rules in the SCC apply if the entity, to whom the data is transferred, is a processor
8 established outside the EEA. The fact that the importer processes the data on behalf of the controller
9 (exporter) justifies the enhanced obligations of the supplier to monitor the compliance of the
10 processor (cf. Principle 33(1)(c)). While the exporter also warrants that it has used reasonable
11 efforts to determine that the importer is able, through the implementation of appropriate technical
12 and organisational measures, to satisfy its obligations under the SCC, the importer shall process
13 the personal data only on documented instructions from the data exporter (Clause 8 Module Two
14 8.1(a)). The may give such instructions on the processing of the personal data throughout the
15 duration of the contract. The SCC also contain rules on the use of sub-processors. Pursuant to
16 Clause 9, the importer may only subcontract any of its processing activities with the written
17 authorisation from the exporter. Where the authorisation has been obtained, the importer shall
18 impose the same obligations on the sub-processor as are imposed on the data importer.

19 A duty to pass on restrictions can also be found in the GDPR (Regulation (EU) 2016/679)
20 for the sub-processing of personal data. According to Article 28(4), when a processor engages
21 another processor to carry out specific processing activities on behalf of the controller, the
22 processor must impose on the sub-processor the same data protection obligations as set out in the
23 contract or other legal act between the controller and the initial processor, either by way of contract
24 with the sub-processor or other legal act under EU or Member State law. These obligations are *inter*
25 *alia* that the processor must process the personal data only on documented instructions from the
26 controller, including with regard to transfers of personal data to a third country or an international
27 organization (Article 28(3)(a)). Furthermore, the processor must make available to the controller
28 all information necessary to demonstrate compliance with the obligations laid down in Article 28
29 and allow for and contribute to audits, including inspections, conducted by the controller or another
30 auditor mandated by the controller (Article 28(3)(h)). However, other than the SCC, the GDPR
31 does not specifically address the onward transfer from one controller to another. Articles 28 and
32 29 contain a series of specific provisions only for controller-to-processor transfers; controller-to-
33 controller transfers are only indirectly covered by the general provisions on data processing. Given
34 that the existence of controller-to-controller transfers cannot have escaped the attention of the
35 European legislator, it will be difficult to apply the detailed requirements which Articles 28 and 29
36 GDPR have established for controller-to-processor transfers simply by analogy (see Christiane
37 Wendehorst, Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data
38 Economy?, in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds.), Data as Counter-
39 Performance – Contract Law 2.0?, 2020, p. 191, 217 ff.).

40 A slightly different approach was taken in the recently proposed Data Governance Act
41 (DGA, COM(2020) 767 final), which sets out conditions for the re-use of protected data held by
42 the public sector. The DGA does not put forward an explicit obligation that a re-user, who intends
43 to transfer public sector data that is confidential or protected by intellectual property rights to a
44 third country, must pass on any restrictions to the recipient. However, Article 5(10) stipulates that
45 the public sector body shall only transmit protected data to a re-user who intends to transfer the
46 data to a third country if the re-user undertakes to comply with the obligations imposed by
47 intellectual property law or confidentiality agreements even after the data is transferred to a third

1 country. Furthermore, the re-user also needs to accept the jurisdiction of the courts of the Member
2 State of the public sector body regarding any dispute related to the compliance with this obligation.
3 This rule does not apply if the re-user transfers the data to a third country that has been declared to
4 provide similar protection of trade secrets and intellectual property (Article 5(9)). In essence,
5 Article 5(10) establishes strict liability of the re-user of public data for any violations of trade secret
6 or intellectual property protection by a downstream recipient that is located in a non-EEA country.
7 While re-users of publicly held data are not explicitly required to pass on restrictions, they will
8 likely do so in order to reduce the risk of being exposed to liability claims. The Proposal deviates
9 from Principle 33 because under the latter the supplier would not be liable for any breaches of a
10 recipient if the supplier passed on its duties and restrictions to the recipient and took reasonable
11 and appropriate steps to ensure compliance with these restrictions.

12 *d. Duty to monitor and remediate wrongful activities.* A duty to inform the recipient of the
13 transferred data that is similar to the one stated in Principle 33(2) can be found in the GDPR
14 (Regulation (EU) 2016/679). According to Articles 16 to 18, data subjects have the right to request
15 the rectification, erasure and restriction of further processing of their personal data. The controller
16 which receives such a request is, pursuant to Article 19, under an obligation to communicate the
17 request to each recipient to which the personal data has been disclosed. A controller is exempted
18 from this obligation, if such communication proves impossible or involves disproportionate effort
19 (cf. Principle 33(2)(b)). Furthermore, Article 17(2) obligates controllers which have made personal
20 data public to take reasonable steps, taking account of available technology and the cost of
21 implementation, to inform controllers which are processing the personal data that the data subject
22 has requested the erasure by such controllers. Once the information reaches the recipient, that
23 recipient is not automatically obligated to comply with the request, as the processing may still be
24 justified by a separate legal ground. (see Christiane Wendehorst, Personal Data in Data Value
25 Chains – Is Data Protection Law Fit for the Data Economy?, in Sebastian Lohsse, Reiner Schulze
26 and Dirk Staudenmeyer (eds.), *Data as Counter-Performance – Contract Law 2.0?*, 2020, p. 191,
27 209 ff.).

28 **Principle 33: Direct action against downstream recipient**

29 **Where an immediate recipient of data had a duty under Principle 32 vis-à-vis its supplier**
30 **to impose particular terms on a downstream recipient to whom the immediate recipient**
31 **will supply the data, and where the immediate recipient has complied with that duty but**
32 **the downstream recipient breaches the terms imposed on it, the initial supplier may**
33 **proceed directly against the downstream recipient after giving notice to the immediate**
34 **recipient.**

35 **Comment:** Where data is passed on by the immediate recipient, two relationships result:
36 one between the initial supplier and its recipient and one between that recipient, now acting as a
37 supplier, and the downstream recipient. It is useful to distinguish between those two relationships
38 in which non-compliance may occur. If the immediate recipient passed the data on to the

1 downstream recipient in breach of terms imposed on it under Principle 32, the immediate recipient
2 is accountable for the wrongful data activities, without prejudice to any additional accountability
3 of the downstream recipient under Principle 34.

4 **Illustration:**

5 144. Assume that business Y in Illustration no. 134 has concluded a valid contract with
6 airline X that defines, inter alia, the conditions under which Y may pass the data
7 harvested from X's website on to third parties. These conditions provide that Y may
8 transfer the data only to third parties within its own group of companies, and that where
9 Y does so Y is under a duty to impose the same condition on the third party. Where Y,
10 in breach of the contract with X, transfers the data to agency Z outside Y's group of
11 companies, this is an issue between the immediate contracting parties X and Y. Z is not
12 liable unless its conduct – such as a failure to act in good faith – creates a separate
13 ground of liability.

14 Where, on the other hand, the immediate recipient fulfills all its duties under Principle 32
15 and imposes the restrictions on the downstream recipient plus takes all other steps that may be
16 required in the circumstances, but then, unforeseeably, the downstream recipient is non-compliant,
17 the immediate recipient has done all that could be expected from it. Subject to any strict vicarious
18 liability under Principle 32(3), the supplier is not liable, but Principle 33 allows the initial supplier
19 to enforce directly against the downstream recipient.

20 **Illustration:**

21 145. Where, in a scenario such as the one described in Illustration no. 144, agency Z does
22 belong to Y's group of companies and the contract between Y and Z does impose on Z
23 the duty to refrain from passing the data on to fourth parties outside the group of
24 companies, but where Z then breaches this duty owed to Y, this is a case for Principle
25 33. In this case, X would have direct remedies against Z.

26 In many jurisdictions, taking direct enforcement action against the downstream recipient is
27 already possible under a range of doctrines, such as concepts of implied assignment (of claims the
28 immediate recipient has against the third party), constructive trust, subrogation to a claim for
29 damages, or, where available, treatment of the supplier as a third-party beneficiary of its immediate

1 recipient's contract with the downstream recipient. Principle 33 advises that the law should seek to
2 achieve this result. The requirement that the initial supplier first give notice to the immediate
3 recipient may be seen as similar to notice requirements in some types of derivative law suits. Unlike
4 derivative law suits, however, any recovery awarded in such a direct action is normally for the
5 benefit of the initial supplier.

6 Principle 33 does not address defences that the downstream recipient would be able to raise
7 against its immediate supplier. Normally, the downstream recipient may also raise such defences
8 against the upstream supplier. However, there may be some doctrines external to these Principles
9 that bring about a different result in some cases.

10 REPORTERS' NOTES:

11 U.S.:

12 For U.S. law regarding third-party beneficiaries, see generally Restatement (Second) of
13 Contracts, §§ 302-15.

14
15 A third party may recover for the breach of a contractual promise if both parties intended to
16 recognize a right to performance in the third-party and either the performance of the promise will
17 satisfy an obligation of the promisee to the beneficiary or the promisee intended to give the benefit
18 of said performance to that third-party. Restatement, Second, Contracts § 302. In the absence of
19 such intent, some states will not allow recovery by third-party beneficiaries. See, e.g., *Katz v.*
20 *Pershing, LLC*, 672 F.3d 64, 73-74 (1st Cir. 2012). Contractual provisions reserving enforcement
21 to other parties may bar even expressly intended beneficiaries bringing suit. See, e.g., *In re TJX*
22 *Cos. Retail Sec. Breach Litig.*, 524 F. Supp. 2d 83, 88-90 (D. Mass. 2007). When manifestations
23 of intent are unclear, overriding social policies, which may be embodied in statutes, may require
24 giving third parties the right to enforce contractual rights without regard to the intention of the
25 parties. Restatement, Second, Contracts Introductory Note to Chapter 14 and § 302 Comment *d*.

26 In the absence of an express non-assignment provision, contractual rights may generally be
27 assigned to third parties unless such assignment would violate statute or public policy, materially
28 change the obligor's duty, or have a materially detrimental effect on the obligor's expectations
29 (such as by increasing the burden imposed upon him or reducing his value received). Restatement,
30 Second, Contracts § 317(2); U.C.C. § 2-210(2). Equity may also permit third-party enforcement
31 by construing contracts making downstream transfers of an asset to include an implied assignment
32 of restrictions contained in the contract effecting the initial transfer. Charles I. Giddings, *Restriction*
33 *Upon the Use of Land*, 5 HARV. L. REV. 274, 284 (1892).

34 Courts may also use their equitable powers to treat a party that is unjustly enriched by its wrongful
35 acquisition of an asset as holding that asset in constructive trust for the equitable owner of the asset,
36 particularly when the asset has special value for the claimant, when it has appreciated, or when its
37 value is difficult to establish. Restatement, Third, Restitution and Unjust Enrichment § 55(1) and
38 Comment *c*.

1

2

Europe:

3 Direct actions vis-à-vis a downstream party within a contractual value chain can be
4 achieved by assigning the immediate recipient's claims against the downstream recipient to the
5 supplier. In general, European contract law allows not only the assignment of present claims but
6 also of future claims that arise out of an existing contractual relationship. However, there are some
7 restrictions, for example, where the assignment would be against public policy or where the rights
8 are personal to the creditor (see Hein Kötz, *European Contract law*, 2nd Edition, 2017, pp. 342 ff.).
9 The assignment of claims usually transfers the rights to performance in respect of the claim
10 assigned as well as all accessory rights securing such performance and would thus also cover
11 remedies in case of non-performance (see Chapter 11 Principles of European Contract Law
12 (PECL); Article III. – 5:101 ff Draft Common Frame of Reference (DCFR)).

13 Another possibility that would lead to a direct action by the supplier against the downstream
14 recipient under Principle 34 is to conclude a contract in favour of a third party, i.e. the immediate
15 recipient and the downstream recipient agree that the supplier may require performance against the
16 downstream recipient (cf. Article 6:110 PECL; Article II. – 9:301 DCFR). Under such a contract
17 the third party, i.e. the supplier, has the same rights to performance and remedies for non-
18 performance as if the downstream recipient were bound to render the performance under a binding
19 unilateral undertaking in favour of the supplier (Article II. – 9:302 DCFR). However, the
20 downstream recipient may assert against the supplier all defences which the downstream recipient
21 could assert against the immediate recipient. For a long time, it was disputed whether contracts in
22 favour of a third party would need the consent of the third party or not. Under most European
23 jurisdictions consent of the third party is not required but the third party may reject the right or
24 benefit (see Article II. – 9:303 Draft Common Frame of Reference (DCFR); Section 881 Austrian
25 Civil Code; Section 333 German Civil Code or Section 141 I(3) French Civil Code; see also Section
26 1 of the Right of Third Party Act 1999 in the United Kingdom).

27 Under French law, direct actions in contractual value chains can be taken by means of the
28 'action directe' in so called 'chaînes de ventes' ('sales chains'). The 'action directe' is based on an
29 early judgement of the Cour de Cassation where the court ruled that a warranty attached to a
30 contract of sale could pass on to the next buyer when the item was resold (Cass. civ., 25 January
31 1820, S. 1820, 1, 171). Thus, if A sells a good to B, and B sells this good to C, C could rely on the
32 warranty attached to the first contract and bring a claim for breach of a contractual warranty against
33 A. The legal nature of the 'action directe' is still disputed. While some authors argue that the
34 warranty claims are transferred along with the thing which is being sold as an accessory (see Jean-
35 Sébastien Borghetti, *Breach of Contract and Liability to Third Parties in French Law: How to Break
36 the Deadlock?*, 2010 *Zeitschrift für Europäisches Privatrecht*, p. 279, 285 ff), others argue that the
37 claims are (tacitly) assigned (see Hein Kötz, *European Contract law*, 2nd Edition, 2017, 329 ff.).
38 The main difference between the French 'action directe' and the direct action under Principle 34 is
39 that the two actions are enforced in opposite directions along the contractual chain. Under the
40 'action directe' the last buyer of a good can act directly against the initial seller (up the contractual
41 chain), while under Principle 34 the initial supplier of data can act against any downstream recipient
42 (down the contractual chain).

43 Direct contractual actions under Principle 33 should not be confused with so-called
44 vicarious liability, under which agents are liable for the actions of their auxiliaries (see Art 6:102
45 of the Principles of European Tort Law). Such vicarious liability can also be found in Article 28(4)
46 GDPR with regard to sub-processing contracts. Where the sub-processor fails to fulfil its data

1 protection obligations, the initial processor shall remain fully liable to the controller for the
2 performance of the other processor's obligations.

3 **Principle 34: Wrongfulness taking effect vis-à-vis downstream recipient**

4 **(1) In addition to wrongfulness following directly from Chapter A, a data activity by a**
5 **downstream recipient that has received the data from a supplier is wrongful where (i)**
6 **control by that supplier was wrongful, (ii) that supplier acted wrongfully in passing the**
7 **data on, or (iii) that supplier acted wrongfully in failing to impose a duty or restriction**
8 **on the downstream recipient under Principle 32 that would have excluded the data**
9 **activity, and the downstream recipient either**

10 **(a) has notice of the wrongfulness on the part of the supplier at the time when the data**
11 **activity is conducted; or**

12 **(b) failed to make such investigation when the data was received as could reasonably be**
13 **expected under the circumstances.**

14 **(2) Paragraph (1) does not apply where**

15 **(a) wrongfulness on the part of the supplier was not material in the circumstances and**
16 **could not reasonably be expected to cause material harm to a party protected under**
17 **Chapter A;**

18 **(b) the downstream recipient obtained notice only at a time after the data was supplied,**
19 **and the downstream recipient's reliance interests clearly outweigh, in the**
20 **circumstances, the legitimate interests of a party protected under Chapter A; or**

21 **(c) the data was generally accessible to persons that normally deal with the kind of**
22 **information in question.**

23 **(3) Paragraphs (1) and (2) apply, with appropriate adjustments, to data activities by a party**
24 **that has not received the data from a supplier but that has otherwise obtained access to**
25 **the data through another party.**

26 **Comment:** *a. General observations.* Principle 34 deals with the situation where data is
27 supplied to a downstream recipient and where there is a protected third party within the meaning

1 of Chapter A, but where the rights interfered with do not directly take effect vis-à-vis the
2 downstream recipient. This could be the case, for example, where an upstream supplier has made
3 data available to an immediate recipient only under contractual limitations within the meaning of
4 Principle 30 and the immediate recipient then wrongfully passed the data on to a downstream
5 recipient without those restrictions, or where a party's data had been accessed by unauthorized
6 means within the meaning of Principle 31 and the 'data thief' then sold the data to a downstream
7 recipient. In all these cases, the immediate recipient or thief would of course be acting wrongfully,
8 but Principle 34 defines the conditions under which data activities by the downstream recipient are
9 also wrongful.

10 Under many legal systems, a third party could become liable vis-à-vis a protected party
11 (such as an upstream supplier) where the third party has or gains knowledge of the fact that the
12 data was obtained through a breach of contract. Liability of the third party would usually be in tort,
13 such as under tortious interference and equivalent concepts. The rationale would normally be that
14 the third party, directly or indirectly, instigated the second party to breach its obligations vis-à-vis
15 the first party or otherwise took part in the wrong committed by the second party vis-à-vis the first
16 party. Such third-party liability may be 'weak' (e.g. there is liability only where the third-party had
17 positive knowledge of the wrong, and only where knowledge was present at the time of the initial
18 acquisition) or 'strong' (e.g. there is also liability where the third party was acting negligently, and
19 also where the third party continued the activities after learning the truth at a point in time after
20 the initial acquisition).

21 Principle 34 is essentially of tort law logic and has opted for a rather 'strong' form of third-
22 party liability, which goes beyond what we find in most legal systems, in the context of interference
23 with contract in general, but remains clearly below what we usually find in the context of
24 interference with tangible property. The solution suggested is similar to a solution that is not
25 uncommon in trade secrets law. This is a policy choice made by these Principles, which seek to
26 strike a balance between the legitimate interests of downstream recipients and those of any
27 protected parties.

28 Principle 34 is without prejudice to Chapter A, i.e. where a data activity by a downstream
29 recipient is already wrongful because the downstream recipient was acting in violation of its own
30 contractual duties, or was itself violating applicable standards of data privacy/data protection law,
31 this is and remains wrongful under Chapter A.

1 *b. Conditions for wrongfulness.* According to paragraph (1), data activities by a downstream
2 recipient may be wrongful even where there is no direct wrongfulness under Chapter A on the part
3 of the downstream recipient itself, but where such wrongfulness was present on the part of the
4 supplier from whom the downstream recipient received the data and either the downstream
5 recipient has notice of the wrongfulness on the part of the supplier at the time when the downstream
6 recipient conducts the relevant data activity or the downstream recipient failed to make such
7 investigation, at the time when the data was received, that could reasonably be expected under the
8 circumstances.

9 For instance, this supplier may have obtained the data by hacking another party's server,
10 i.e. control by the supplier itself may already have been wrongful as such.

11 **Illustration:**

12 146. Start-up company S is developing a new robot. For 'training' the robot's intelligent
13 software S would need huge amounts of industry data which the controllers of the data
14 are either not prepared to make available to S or are offering at a price S cannot afford.
15 Fortuitously S is offered suitable data at an affordable price from backstreet business B,
16 and without asking questions about how B got the data, S makes the deal and uses the
17 data for training the robot. If B had gained control of the data by hacking other people's
18 servers, S was not rightfully in control of the data, because S had failed to make the
19 investigations that could reasonably be expected under the circumstances when buying
20 the data.

21 Even if the supplier was rightfully in control of the data the supplier may not have been
22 allowed to pass the data on to the downstream recipient, for example, because of a contractual
23 limitation under Principle 30. Even where the supplier was allowed to pass the data on to the
24 downstream recipient the supplier may have been under an obligation to impose restrictions on the
25 downstream recipient under Principle 32 and may have failed to do so. In all these cases the supplier
26 would have been acting wrongfully, but, if it were not for Principle 34, this would not mean that
27 wrongfulness on the part of the supplier affects data activities by the downstream recipient.

28 **Illustration:**

29 147. Assume that B in Illustration no. 146 had not hacked other people's servers, but was a
30 data trustee within the meaning of Principle 13 who had promised to the entrusters not

1 to make the data available to third parties within a defined range of industries (including
2 the industry to which S belongs) because that might harm the economic interests of the
3 entrusters. If S had (or later gains) notice of this restriction or had failed to make the
4 investigations that could reasonably be expected under the circumstances at the time the
5 deal with B was made, and nevertheless continues its data activities, S is acting
6 wrongfully.

7 The level of care that can be expected from a downstream recipient is higher at the point in
8 time when the downstream recipient acquires the data, at which time the downstream recipient
9 must take reasonable and appropriate steps to ascertain whether the supplier was acting rightfully.
10 These Principles do not define the precise steps required in each kind of scenario. Generally
11 speaking, a risk-based approach is also to be applied in this context. The less information the
12 downstream recipient has about the supplier and the original data sources, the less indications there
13 are that the supplier is trustworthy, the higher the probability that there are restrictions within the
14 meaning of Chapter A and the higher the potential risk for protected parties, the more inquiries a
15 downstream recipient can be expected to make.

16 **Illustration:**

17 148. In Illustration no. 146 a court would consider that S was well aware that the ‘regular’
18 controllers of the data were normally unwilling to make them available, so if B suddenly
19 turned out to be in control of such data, in particular as a ‘backstreet’ type of business,
20 this was already more than enough reason for S to be on the alert. In such a situation S
21 should have made rather thorough inquiries. If, on the other hand, S had made a deal
22 directly with company C whose machines generate the industry data, the probability
23 that another party has a better right to the data than C would have been rather low, as
24 would have been the burden on S to make further inquiries.

25 Even where the downstream recipient has made the investigations that could reasonably be
26 expected under the circumstances at the time when the acquisition was made, actual notice obtained
27 at a point in time after the data was acquired may still render data activities wrongful, but only for
28 the future. The downstream recipient that obtains notice must stop the relevant data activities.

1 c. *Protection for downstream recipients.* The rule in paragraph (1) is potentially quite far-
2 reaching and may entail rather high risks for downstream recipients. This is why the rule needs to
3 be restricted in a number of cases, which are listed in paragraph (2).

4 The rationale of paragraph (2)(a) is that of a *de minimis* rule. With data, a multitude of
5 restrictions could follow from all sorts of directions, including, in particular, very detailed data
6 privacy/data protection regulation and a host of very far-reaching restrictions imposed by
7 contractual means as a matter of routine in standard contract terms. These restrictions could
8 accumulate, with the possibility that the data would also be ‘tainted’ for onward recipients. If
9 onward transferees were subject to all such accumulated restrictions, this could add significant risk
10 to the data economy because there would be no such thing as ‘untainted’ data any more.
11 Accordingly, some sort of rule protecting transferees is necessary in order to avoid over-detering
12 data transfers. Despite notice of some kind of wrongfulness on the part of the supplier, a
13 downstream recipient should still not be acting wrongfully if the wrongfulness on the part of the
14 supplier (of which the recipient has notice) is not material and could not reasonably be expected to
15 cause material harm to protected third parties.

16 **Illustrations:**

17 149. Real property business R hires the services of company D to create digital twins of R’s
18 buildings to facilitate maintenance. The data is to be transferred to R in order to enable
19 R to respond where repair is needed. D clandestinely sells some of this data to local
20 tourist guide organisation T because some of the photos include a wonderful view of
21 the beach at sundown. This may be in breach of the contract D has with R, as D may
22 not be allowed under this contract to pass data on to third parties, but under the given
23 circumstances this breach is not material and cannot really cause harm to R (assuming
24 that making the deal with T himself would never have crossed R’s mind and R does not
25 lose a business opportunity, and that R does not have copyright in the material). So T
26 would be allowed to keep the photos even if T had been perfectly aware of how D
27 obtained the photos (but any liability on the part of D would remain unaffected).

28 150. If D in Illustration no. 149 instead sells the photos to X, who runs a database that seeks
29 to warn potential buyers of immovable property against buying premises that are in bad
30 shape, this obviously may harm R’s interests, so notice on the part of X that D acted
31 wrongfully clearly makes control by X wrongful.

1 Generally speaking, a case-by-case assessment needs to be made to decide whether or not
2 a violation or breach on the part of the supplier is material. In doing so, one must take into account,
3 in particular, the significance of the duty breached for the legitimate interests of the protected party
4 and whether the supplier was acting purposely, recklessly, negligently or innocently. As far as
5 contractual restrictions within the meaning of Principle 30 are concerned, cautious analogies could
6 be drawn to doctrines relating to material breach of contract. Unauthorized access within the
7 meaning of Principle 31 would usually be considered to be material, but there may be exceptions,
8 for example, where security measures taken were very weak and it would not be justified to assume
9 downstream third-party effects. In assessing potential harm to the protected party, an objective
10 standard seems appropriate.

11 **Illustration:**

12 151. In Illustration no. 149 above, if R subjectively feels uneasy about one of his buildings
13 being visible on a photo used by a tourist guide company, that would not be sufficient
14 to make control by T wrongful. Control by T would be wrongful even without any
15 objective risk of harm only if, in the contract between R and D, this had been
16 specifically highlighted as important, thus making the breach by D a material breach.

17 Paragraph (2)(b) is an exception from paragraph (1) for downstream recipients who
18 exercised due diligence when acquiring the data and who have taken further steps and made further
19 investment in reliance on the acquisition of the data. While the downstream recipient's reliance
20 cannot generally outweigh the legitimate interests of the protected third party, there may be
21 situations where, on balance, the downstream recipient's interests should take priority.

22 **Illustration:**

23 152. R acquires large amounts of data required for training a new AI from S at a price of
24 several million USD. When making the deal with S, R diligently checks the relevant
25 documents made available to it and makes all enquiries about the origin of the data that
26 can reasonably be expected, and S provides representations and warranties that it has
27 the legal right to sell the data. In reliance on the availability of the data, R invests another
28 several million USD in the development of the AI. Three years later it becomes apparent
29 that, for reasons R could not reasonably have detected, S was actually not allowed to
30 sell the data to R because of an unexpected third party claim from S's parent company

1 P. In this case, a court should take into account the huge economic harm R would suffer
2 if it must stop using the data, that R had been acting diligently, and that P should have
3 monitored the activities of its subsidiaries to make sure its rights were not infringed. A
4 court might thus, in this case conclude that R’s legitimate interests outweigh those of P
5 and S and that R may continue using the data.

6 Last but not least, a downstream recipient’s data activities should not be considered
7 wrongful where the information was generally accessible to persons within circles that normally
8 deal with the kind of information in question.

9 **Illustration:**

10 153. Through unauthorized access to C’s servers, S obtains access to a number of chemical
11 formulas associated with patents held by C and sells the data to R. The chemical
12 formulas are available to any interested party from the patent office, and have
13 subsequently been published in scientific journals. In this situation, processing of the
14 chemical formulas by R should not be considered wrongful even if R was aware of how
15 S had obtained access to the data, because R could, at any time, have made the effort to
16 obtain the data from the patent office or from scientific journals.

17 *d. Application to similar situations.* There are some situations in which the conditions of
18 paragraph (1) are not strictly fulfilled because there was no supply, but it would still be appropriate
19 to apply the same rules. This is why paragraph (3) provides that paragraphs (1) and (2) apply with
20 appropriate adjustments to data activities by a party that has not received the data from a supplier
21 but has obtained access to the data through another party.

22 **Illustration:**

23 154. Parent company P has supplied data to subsidiary S, explicitly prohibiting any onward
24 transfer to third parties without the explicit consent of P. After R has not succeeded in
25 persuading S to sell R the data, R hacks S’s servers and obtains unauthorized access to
26 the data. S then becomes insolvent and is no longer able to take action against R, or no
27 longer interested in doing so. However, while the data has not been ‘supplied’ to R by
28 S, data activities by R are not only wrongful vis-à-vis S, but also vis-à-vis P.

1 **REPORTERS' NOTES:**

2 **U.S.:**

3 Current law on tortious interference with contract incorporates what the Comment calls 'weak'
4 third-party liability, which requires intent. Restatement, Third, Torts: Liability for Economic Harm
5 §§ 7(b), 17(1)(d)-(e). Courts have required intentional conduct when evaluating claims of tortious
6 interference with rights to data. See 3D Glob. Sols., Inc. v. MVM, Inc., 552 F. Supp. 2d 1, 9-10
7 (D.D.C. 2008). Other courts have similarly refused to allow claims based on mere negligence for
8 data security breaches that caused purely economic losses. See *In re TJX Cos. Retail Sec. Breach*
9 *Litigation*, 524 F. Supp. 2d 83, 90-91 (D. Mass. 2007). The law of restitution may also permit
10 recovery of gains obtained by a party that interfered with business relations. Restatement, Third,
11 Restitution and Unjust Enrichment § 44. Equitable remedies, such as constructive trusts, are not
12 available for the conduct of bona fide purchasers prior to their receiving notice of the potential
13 wrongfulness of their possession of the asset in question. Restatement, Third, Restitution and
14 Unjust Enrichment § 66.

15 As the Comment notes, the endorsement of 'strong' third-party liability represents a policy choice
16 largely derived from trade secret law, which imposes liability for uses or disclosures of trade secrets
17 that actors know or have reason to know were wrongfully obtained. Restatement, Third, Unfair
18 Competition § 40(b); Uniform Trade Secrets Act § 1(2)(ii)(B)(III). Trade secret law does not
19 provide immunity for onward transferees that obtain knowledge of wrongfulness after the time of
20 transfer, although it bases the determination of monetary relief on factors such as the fact and extent
21 of pecuniary losses and gains, the nature and extent of the appropriation, and good faith reliance,
22 among other things. Restatement, Unfair Competition § 45(2); Uniform Trade Secrets Act § 3
23 Comment. In addition, trade secret law may not require defendants to relinquish all profits when
24 they have made good-faith investments in the trade secret prior to receiving notice of the plaintiff's
25 claim. Restatement, Unfair Competition § 45 Comment g; Uniform Trade Secrets 3(a). Injunctive
26 relief similarly depends on the nature of the interest and the appropriation, the likely harm, and
27 good faith, among other factors. Restatement, Unfair Competition § 44(2); Uniform Trade Secrets
28 Act § 2 Comment. Unqualified injunctive relief may not be appropriate when good-faith defendants
29 have made substantial investments in reliance on the trade secret prior to notice that it had been
30 misappropriated. Restatement, Unfair Competition § 43 Comments b-c; Uniform Trade Secrets
31 2(b). This approach rejects the one taken in Restatement, First, Torts § 758(b), which accorded
32 absolute immunity to good faith transferees.

33 **Europe:**

34 As contractual rights are relative in nature, they can only be infringed by persons who owe
35 a corresponding obligation to the holder of the right. An exception to this fundamental principle is
36 the inducement of non-performance of a contractual obligation, which gives rise to non-contractual
37 liability under all European jurisdictions and previously existed in Roman law. The underlying
38 rationale is that where a third party intentionally induces a person not to perform contractual or
39 other obligations to another party, this party who thereby suffers loss may claim reparation from
40 the person inducing the non-performance (see Article 2:211 Principles of European Law – Non-
41 Contractual Liability Arising out of Damage Caused to Another; Article 2:211 Draft Common
42 Frame of Reference (DCFR)). In some European legal systems, liability not only arises where a
43 person intentionally induces the infringement of an obligation but also where they know or should
44 have known of the breach of the obligation.

1 For example, under French law, a tortious *faute* is committed if a person knowingly aids
2 another person in breaching a contractual obligation. Liability arises vis-à-vis the party who is
3 affected by this breach of contract, and it suffices that the person inducing the breach had
4 knowledge of the existence of the contract (Cass.civ. 17, Bull.civ. 2000, I, no. 246 p. 161). In
5 Austria, it is undisputed that inducing a breach of contract with the intention to cause harm
6 constitutes an immoral infliction of damage under Section 1295(2) Austrian Civil Code (ABGB).
7 Liability also arises where such intention to harm does not exist (or cannot be proven) but a person
8 had knowledge of the contractual obligation and deliberately influenced the will of the contracting
9 party to breach the contract (see Austrian Supreme Court, Case 7 Ob 225/03v). According to the
10 Austrian Supreme Court, in cases in which the initial buyer of an immovable object is not yet the
11 owner but already possesses the property, any secondary buyer becomes liable if they should have
12 known that the seller is breaching its contract (see Austrian Supreme Court, Case 2 Ob 126/13p).
13 However, the second buyer is only required to perform a limited amount of due diligence, as
14 otherwise commercial transactions would be severely impaired. Liability for inducing the non-
15 performance of an obligation is more restricted under German law. According to the prevailing
16 view, the general clause in German tort law, Section 823(1) German Civil Code (BGB), only
17 protects absolute rights. Hence, mere knowledge of a contractual obligation (which is a relative
18 right) does not lead to liability for inducement of breaching an obligation. Only where the breach
19 of contract was induced intentionally to cause harm to the contracting party and against good
20 morals does liability arise according to Section 826 BGB.

21 While the level of care expected from downstream recipients of data under Principle 34
22 goes beyond the protection of contractual rights, it is significantly lower than the protection of
23 absolute rights, such as ownership, which need to be respected by any third party. Other than under
24 Principle 34, the transferee of a movable object, even if it could not have had knowledge that the
25 seller was not the owner of the sold object, infringes the owner's property rights. There are only a
26 few exceptions, with rather strict requirements, to this general rule, most notably the acquisition in
27 good faith, a doctrine which exists in all European legal traditions and is based on the rationale that
28 the protection of the bona fide acquirer is necessary to ensure the functioning of commercial trade.
29 In Austria, good faith acquisition of moveable goods is regulated in Section 367 of the Austrian
30 Civil Code. The transferee acquires ownership of a good obtained from a person who is not the
31 owner, only if the transferee neither knows nor should suspect that seller is not the owner, and the
32 object is acquired either at a public auction, from a professional trader acting in the course of their
33 ordinary business, or from a person to whom the owner voluntarily entrusted the object
34 ('Vertrauensmann'). In France, transfer of ownership is based on a consensual system. Hence,
35 ownership is transferred as soon as an express agreement to that effect is reached between both
36 parties. Hence, ownership is transferred when an express agreement between both parties is met.
37 In these cases, ownership is not transferred *solo consensus* but instead by mere possession.
38 Excluded from good faith acquisition are stolen and lost goods during a period of three years from
39 the day of the loss or theft (Article 2276(2) French Civil Code). However, if the possessor of a lost
40 or stolen thing has bought it in good faith at a fair, market, public sale, or from a merchant selling
41 similar things, the possessor is only obligated to return the stolen or lost property to the
42 dispossessed owner against reimbursement of the purchase price (Article 2277 French Civil Code).
43 The German rules on good faith acquisition (Sections 932 ff of the German Civil Code) require
44 that the transferee obtained possession and does not know or has no reason to know that the thing
45 does not belong to the transferor. However, good faith acquisition is excluded if the goods were
46 stolen from the owner or otherwise gone missing and have not been bought in the course of a public
47 auction (Section 935).

1 The Trade Secrets Directive (Directive (EU) 2016/943; see also Article 39 of the Agreement
2 on Trade-Related Aspects of Intellectual Property Rights (TRIPS)) also contains rules for onward
3 transfer. These are less strict than the requirements for good faith acquisition but more far reaching
4 than the liability for inducement of non-performance of an obligation. According to Article 4(4),
5 the acquisition, use or disclosure of a trade secret by a person is considered unlawful if the person
6 knew or ought, under the circumstances, to have known that the trade secret had been obtained
7 directly or indirectly from another person who was using or disclosing the trade secret unlawfully
8 within the meaning of Article 4(3) of the Directive. Article 4(3) states that the use or disclosure of
9 a trade secret shall be considered unlawful whenever carried out, without the consent of the trade
10 secret holder, by a person who is found to meet any of the following conditions: (a) having acquired
11 the trade secret unlawfully; (b) being in breach of a confidentiality agreement or any other duty not
12 to disclose the trade secret; (c) being in breach of a contractual or any other duty to limit the use of
13 the trade secret. While Principle 34(1) has certain similarities to Article 4(3), Principle 34(2), unlike
14 the Trade Secrets Directive, states a de minimis rule that limits the wrongfulness of data activities
15 by a downstream recipient. The policy choice to include such a limitation was made because
16 otherwise the protection of trade secrets would unjustifiably be extended to all types of data.

17 Similar effects vis-à-vis downstream recipient can also be found in Articles 2(1)(xii) – (xv)
18 of the Japanese Unfair Competition Prevention Act. The provisions declare the act of disclosing
19 shared data with limited access after having acquired it and learning that there had been an
20 intervening act of wrongful acquisition of shared data with limited access as ‘unfair competition’.
21 The same holds true for the act of using or disclosing the data that has been disclosed by an
22 undertaking holding that data for the purpose of wrongful gain or causing damage to that holder of
23 shared data with limited access. In addition, the act of acquiring shared data with limited access
24 with the knowledge that the disclosure of that data is an act of improper disclosure of shared data
25 with limited access or that there has been an intervening act of improper disclosure of shared data
26 with limited access with regard to the relevant shared data with limited access, or the act of using
27 or disclosing shared data with limited access acquired in such a way, is declared as unfair
28 competition.

29 With regard to subsequent knowledge of unlawful activities, the rule laid down in the Trade
30 Secrets Directive is also similar to paragraph 2(b). According to Article 4(4) Trade Secrets
31 Directive, unlawfulness of the acquisition, use or disclosure is always determined ‘at the time of
32 the acquisition, use or disclosure’. Therefore, once the recipient knows or ought to know that the
33 trade secret had been obtained directly or indirectly from another person who was using or
34 disclosing the trade secret unlawfully, any further use becomes unlawful. Similarly, Article
35 2(1)(xvi) of the Japanese Unfair Competition Prevention Act qualifies the act of disclosing shared
36 data with limited access after having acquired that data and learning that the relevant acquisition
37 falls under an act of improper disclosure of shared data with limited access or that there had been
38 an intervening act of improper disclosure of shared data with limited access, as unfair competition.
39 However, under Principle 34, the subsequent knowledge does not lead to the unlawfulness of data
40 activities by the downstream recipient, if the recipient’s reliance interests clearly outweigh, in the
41 circumstances, the legitimate interests of a party protected under Principles 29 to 31.

1 **Chapter C: Effects of Other Data Activities on the Protection of Third Parties**

2 **Principle 35: Duties of a controller with regard to data processing and derived data**

3 **(1) If a controller may process data but is obligated to comply with duties and restrictions**
4 **within the meaning of Chapter A, the controller must, when processing that data,**
5 **exercise such care that is reasonable under the circumstances in**

6 **(a) determining means and purposes of processing that are compatible with the duties**
7 **and restrictions; and**

8 **(b) ascertaining which duties and restrictions apply with regard to the derived data and**
9 **taking reasonable and appropriate steps to make sure the duties and restrictions are**
10 **complied with.**

11 **(2) Whether duties and restrictions with regard to the original data also apply with regard**
12 **to derived data, or whether lesser or additional duties and restrictions apply, is to be**
13 **determined by the rules and principles governing the relevant source of protection**
14 **under Chapter A. In a case of doubt, considerations to be taken into account include:**

15 **(a) the degree to which the derived data is different from the original data, such as**
16 **whether the original data can be reconstructed from the derived data by way of**
17 **reasonable steps of disaggregation or reverse engineering; and**

18 **(b) the degree to which the derived data poses a risk for a protected party as compared**
19 **with the risk posed by the original data.**

20 **(3) If processing the original data was not wrongful, but subsequent events occur that would**
21 **make the same type of processing wrongful, this does not retroactively make the prior**
22 **processing wrongful.**

23 **Comment:** *a. General observations.* Chapters A and B have addressed the question of when
24 data activities are wrongful vis-à-vis a protected party, assuming that wrongfulness can be
25 established with regard to a particular data set and that this data set remains more or less identical
26 in the course of events, such as when it is supplied to a downstream recipient. In practice, however,
27 this is rarely ever the case. Rather, data is usually subject to processing activities, meaning that data

1 is structured, refined, combined with other data, and new data is derived or inferred from existing
2 data. This makes the legal analysis much more complicated as it is unclear whether or to what
3 extent the ground for wrongfulness is still present in the derived data, and even if it is, investment
4 has been made with respect to the data, and the data ‘tainted by wrongfulness’ have been combined
5 with ‘untainted’ data. There may thus be situations where it would be disproportionate and/or
6 manifestly inefficient to judge data activities with regard to the processed data set in exactly the
7 same way as data activities with regard to the original data set.

8 There are many different ways in which data may be processed. It is arguably not helpful
9 to create different Principles for each typical processing activity, in particular as these activities are
10 usually applied in combination and as the lines between them are blurred. The main types of
11 processing activities relevant for the purposes of Chapter C will be the structuring, aggregation,
12 and analysis of data (including the drawing of inferences from data with the help of probabilistic
13 or similar assumptions).

14 **Illustration:**

15 155. Credit scoring company B uses data it has been provided by and about customer C,
16 who is seeking a loan, in order to obtain, with the help of a very complex algorithm, a
17 figure representing C’s credit score. Various steps may be involved here. Assuming B
18 has collected data about C from various different sources and has combined and
19 commingled them in sophisticated ways (e.g. representing, in a structured way, all
20 information about C’s conduct in the context of paying bills), this is aggregated data.
21 Where B has analyzed the input data and derived certain statistical data from it (e.g. that
22 it took C, on average, 24 days to pay a bill that was due), this is derived data. Where B
23 then obtains the final credit score with the help of numerous probabilistic assumptions
24 embedded in B’s algorithm (e.g. that persons of C’s age who take an average of 24 days
25 to pay a bill, live in C’s neighborhood, hold the same number of bank accounts and
26 mobile phones as C does, and buy as much alcohol and coffee as C seems to be doing
27 according to payment services data, have a 34 percent probability of defaulting), B is
28 generating inferred data. The aggregated, derived and inferred data all constitute
29 ‘derived data’ within the meaning of Principles 3(1)(h) and 35(1).

30 Often, data is used in such a way that inferences are drawn, but no inferred data is created
31 and stored anywhere, so no inferred data seems to exist. Rather, the inference is drawn ad hoc with

1 the help of an algorithmic system, immediately triggering a reaction. This must have the same
2 effect as if inferred data had been collected and stored.

3 **Illustration:**

4 156. In a scenario like the one described in Illustration 155, credit rating company B may in
5 fact never calculate C's credit score (and store it in their system, later basing a
6 recommendation to reject C's application for a loan on this score), but may instead
7 apply an algorithm that, with the help of all the input data B has about C, automatically
8 triggers the sending of a rejection letter. There are various reasons why B may prefer to
9 do that, including circumventing data protection law. Nevertheless, the decision
10 represented in the rejection letter would have the same effect as the inferred data and
11 would thus equally be covered by Principle 35(1).

12 *b. Duties of controller when processing.* Any controller that intends to engage in processing
13 of data with regard to which that controller is (or may be) bound by duties and restrictions under
14 Chapters A and B must apply due diligence in making sure that processing the data in the intended
15 way and for the intended purpose is compatible with the duties and restrictions. The level of
16 diligence required depends, once more, on a risk-based assessment, that is, the higher the
17 probability that restrictions may affect the processing, and the higher the potential risk for protected
18 parties from non-compliance, the more inquiries a controller must make and the more safeguards
19 that the controller must put into place.

20 **Illustration:**

21 157. Credit rating company B in Illustration no. 155 not only calculates credit scores of
22 consumers like C but also processes data generated by the smart heating system of its
23 office building in order to cut down on repair and maintenance costs. Evidently, the
24 probability that data processing is subject to restrictions is considerably higher in the
25 case of the consumer data than in the case of the heating system data, and so is the
26 potential risk involved for third parties. Thus, B must apply a considerably higher level
27 of diligence with regard to the consumer data.

28 After processing, the controller also must exercise reasonable care to ascertain which duties
29 and restrictions apply with regard to the derived data. Often, the restrictions will be less strict than

1 with regard to the original data because processing may have removed the basis for protection (e.g.
2 previously personal data may have become anonymized). However, the opposite may also be true,
3 in particular where data from different sources has been combined and risks for protected parties
4 have increased.

5 **Illustration:**

6 158. Credit rating company B in Illustration no. 155 combines data of various types and
7 from various sources, including data from fitness bracelets, step-counting apps, smart
8 refrigerators, and shopping reward systems. All this data is combined for the purpose
9 of making predictions concerning a consumer's health and that consumer's
10 consequential risk of becoming unemployed and defaulting on debts. The health-related
11 data is much more sensitive than was the input data from other sources, so more duties
12 and restrictions might exist for processing the resulting health data than for processing
13 the original data.

14 *c. Prevailing duties and restrictions.* When data undergoes processing, the legal situation
15 with regard to this data changes, including, in particular, with regard to the protection of other
16 parties under Chapter A. Duties and restrictions for the protection of such parties may be the same
17 with regard to the derived data, or they may be lesser, or greater. Principle 35(2) clarifies that the
18 extent of these duties and restrictions is governed by those rules and principles that govern the
19 duties and restrictions regarding the original data, or parts thereof. This is clear in the case of rights
20 within the meaning of Principle 29, which are governed by particular bodies of law with their own
21 inherent logic and principles.

22 **Illustration:**

23 159. Whether derived data in Illustration no. 155 counts as anonymous statistical data (such
24 as the percentage of consumers living in a particular community defaulting on their
25 debts) outside the scope of data protection law and without any restrictions on
26 processing, or within the scope of such law, is to be determined exclusively by the
27 applicable data protection law itself. The same holds true for the question of whether
28 the health-related data in Illustration no. 158 is subject to stricter privacy rules and what
29 these rules are.

1 However, the same holds true where limitations originate from contract within the meaning
2 of Principle 30, in which case the exact scope of such limitations, and whether or not they extend
3 to derived data, must normally be ascertained by way of contract interpretation.

4 **Illustration:**

5 160. Manufacturer M of machines transfers machine performance data to supplier C of an
6 important component. C may not disclose ‘the data’ to third parties. C processes the
7 machine performance data and derives from that data, inter alia, data concerning the
8 accuracy of performance measurement in general (which does not refer specifically to
9 a particular type of machine). Whether this derived data is still covered by the
10 contractual restriction on disclosing data to others, or whether this data is so different
11 from the original performance data that C is free to use this data, is to be determined by
12 contract interpretation.

13 *d. Considerations in case of doubt.* There may be cases where the rules or principles
14 ordinarily governing restrictions within the meaning of paragraph (1) are silent, or where there are
15 different possibilities of interpretation, in which case the default rule in paragraph (2) applies.
16 Under this default rule, there are two cases where duties and restrictions with regard to the original
17 data, or part thereof, prevail with regard to derived data.

18 The first case is where the original data can, by reasonable reverse engineering, be
19 reconstructed from the derived data. If the original data is more or less included in the derived
20 data, the derived data obviously bears more or less the same inherent risks for protected parties as
21 did the original data. The second case is where the duties and restrictions must be applied to the
22 derived data to prevent harm to a party protected under Chapter A. The harm need not be exactly
23 the same kind as the harm that might have followed from the original data.

24 **Illustration:**

25 161. Assume that the contract in Illustration no. 160 is silent about the use of derived data,
26 and a court needs to fill the gap. If a court concludes that disclosure of this data to third
27 parties would not cause relevant harm to M, C may disclose this data to third parties.

28 *e. Subsequent grounds for wrongfulness.* Paragraph (3) of Principle 35 deals with situations
29 where processing data was rightful at the time it took place, but subsequent events make the same

1 type of processing wrongful. Subject to any specific rule of law that exceptionally takes priority
2 and provides for retroactive effect, these Principles suggest that such subsequent events should not
3 normally affect the rightfulness of the processing. However, the subsequent events may mean that
4 the derived data is affected by the same grounds of wrongfulness, so any duties and restrictions
5 that follow directly from Chapter A with regard to the derived data may be relevant and mean that
6 the derived data must be deleted.

7 **Illustration:**

8 162. Assume that, under the applicable data protection law, processing of all consumer data
9 in Illustration no. 155 was based on the consumer's consent. Assume further that, under
10 the applicable data protection law, consent may be withdrawn at any time, and data
11 whose control and processing relies exclusively on consent must normally be deleted.
12 If consumer C withdraws consent, this makes future control and any future processing
13 of the original data by B wrongful, but it also affects the derived data as far as this data
14 is still identifiable to C.

15 Whether or not the subsequent grounds of wrongfulness affect the derived data is
16 determined by paragraph (2).

17

18 **REPORTERS' NOTES:**

19 **U.S.:**

20 Issues arising from when assets that are subject to a party's claims are aggregated with
21 other assets raise legal problems in a number of contexts. See, e.g., in the context of security
22 interests, UCC § 9-335 (addressing accessions and stating that security interests may be created in
23 an accession) and UCC § 9-336 (addressing commingled goods and stating that commingled goods
24 may have security interests that do not exist for individual, unbundled goods).

25 Some statutes recognize practical limits on the ability to disaggregate personal information.
26 For example, the California Privacy Rights Act added exemptions to the rights to delete personal
27 information and to opt out of sharing of personal information if the personal information initially
28 received consent and was used to produce a physical item containing the consumer's photograph
29 if the business has incurred expense in reliance on the consumer's initial consent and compliance
30 would not be commercially reasonable. CAL. CIV. CODE § 1798.145(r).

31 **Europe:**

32 *a. General observations.* The processing of data may in many instances lead to the
33 generation of new data. To better illustrate the way in which the new data differs from the initial
34 dataset, attempts have been made to categorize derived data according to the activity that gave rise

1 to it. The terms ‘derived’ data and ‘inferred’ data are often used as synonyms for data that a
2 controller creates by drawing conclusions from provided datasets (see OECD, Enhancing Access
3 to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p.
4 31; METI, Contract Guidelines on Utilization of AI and Data – Data Section, 2018, p. 19; EDPB,
5 Guidelines 8/2020 on the targeting of social media users, Version 1.0, 2 September 2020, p. 22;
6 see also Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP
7 242 rev.01, 5 April 2017, p. 10). Others, however, distinguish between data that has been derived
8 and data that has been inferred. Derived data stems from a mechanical procedure on other data and
9 is a new data element related to the individual. Inferred data implies the drawing of conclusions
10 with the help of probabilistic or similar assumptions. In other words: the former is data that is
11 simply derived in a fairly mechanical fashion from other data. Inferred data is the product of a
12 probability-based analytic process (see Martin Abrams, *The Origins of Personal Data and its*
13 *Implications for Governance*, 2014, p. 7 f.). In practice it may be quite difficult to draw a clear line
14 between derived and inferred data, which probably led to the custom to use these words as
15 synonyms.

16 Another category that is frequently used is that of ‘aggregated data’. While no universally
17 accepted definition for aggregated data yet exists, it usually refers to the combination of initially
18 separated data sets. Data aggregation is an activity that is likely to be conducted by controllers, as
19 the value of the aggregated sets may significantly exceed the sum of values of the separate sets
20 (Bertin Martens et al., *Business -to-Business data sharing: An economic and legal analysis – JRC*
21 *Digital Economy Working Paper 2020-05*, 2020, p. 5, 12). However, the categorization as
22 aggregated data does not indicate whether the combined datasets can, with reasonable effort, be
23 disaggregated.

24 *b. Duties of controller when processing and c. Prevailing duties and restrictions.* Data that
25 results from personal data is typically under the protection of the GDPR (Regulation (EU)
26 2016/679), as long as the derived data still relates to an identified or identifiable natural person and
27 is thus considered personal data within the meaning of Article 4(1) GDPR. In determining whether
28 a natural person is still identifiable, account should be taken of all the means reasonably likely to
29 be used, such as singling out, by the controller or another person to identify the natural person
30 directly or indirectly (see Recital 26 GDPR). Where the derived data stems from data protected by
31 the Trade Secrets Directive (Directive (EU) 2016/943), the infringer is required to destroy the data
32 if it contains or embodies the trade secret (Article 12(1)(d)).

33 *e. Subsequent grounds for wrongfulness* typically do not affect any processing that has been
34 made during the period before those grounds arose. The predominant example is the withdrawal of
35 consent under Article 7(3) GDPR (Regulation (EU) 2016/679). While the data subject is entitled
36 to withdraw his or her consent at any time, the provision explicitly sets out that the withdrawal of
37 consent shall not affect the lawfulness of processing based on consent before its withdrawal.

38 **Principle 36: Wrongful processing**

39 **(1) Where processing data was wrongful, the controller must take all reasonable and**
40 **appropriate steps to undo the processing, such as by disaggregating data or deleting**
41 **derived data, even where duties and restrictions under Chapters A and B do not apply,**
42 **in accordance with Principle 35, with regard to derived data.**

1 **(2) To the extent that undoing the processing in cases covered by paragraph (1) is not**
2 **possible or would mean a destruction of values that is unreasonable in light of the**
3 **circumstances giving rise to wrongfulness on the part of the controller and the legitimate**
4 **interests of any party protected under Chapter A, an allowance may be made in money**
5 **whenever and to the extent this is reasonable in the circumstances and may be combined**
6 **with restrictions on further use of the derived data. Factors to be taken into account**
7 **include**

8 **(a) whether the controller had notice of the wrongfulness at the time of processing;**

9 **(b) the purposes of the processing;**

10 **(c) whether wrongfulness was material in the circumstances or could be expected to**
11 **cause relevant material harm to a party protected under Chapter A; and**

12 **(d) the amount of investment made in processing, and the relative contribution of the**
13 **original data to the derived data.**

14 **(3) Paragraphs (1) and (2) apply with appropriate adjustments to products or services**
15 **developed with the help of the original data.**

16 **Comment:** *a. General observations.* The question of the appropriate legal consequences of
17 wrongful processing of data is one of the most complex issues to be solved in the data economy.
18 Clearly, a balance needs to be struck between, on the one hand, the objective of encouraging
19 negotiations and avoiding incentives for reckless infringement of others' rights (which might exist
20 if a controller could fully keep and use the derived data), and on the other hand the objective of
21 preserving value that has been generated. Under Principle 36, the general rule is that a controller
22 that has engaged in wrongful processing is under an obligation to undo the processing. However,
23 as an alternative, a court may decide that the controller may make a monetary payment to the
24 affected person, if requiring the controller to undo processing would be disproportionate and
25 unreasonable in the circumstances.

26 It is important to understand the relationship between Principle 36 and Principle 35. Where
27 duties and restrictions for the protection of other parties within the meaning of Chapters A and B
28 prevail with regard to the derived data, the legal consequences are those that follow from the
29 relevant duties and restrictions themselves. Principle 36 only comes into play where, under

1 Principle 35, duties and restrictions within the meaning of Chapters A and B do not apply to the
2 derived data and therefore the controller would, but for Principle 36, be allowed to keep the derived
3 data. Principle 36 thus follows a ‘fruit of the poisonous tree’ logic.

4 **Illustration:**

5 163. Social network provider P recklessly uses photographic material and stream recordings
6 generated by its users for developing facial recognition AI. That use is clearly
7 inconsistent with the applicable data protection regime. However, the resulting facial
8 recognition AI does not, as such, qualify as personal data and, thus, is not subject to any
9 restriction following from data protection law. While P may be subject to a fine for
10 having recklessly violated data protection law (if a regulator ever obtains sufficient
11 evidence against P), P would – but for Principle 36 – still be able to use the facial
12 recognition AI, possibly making a fortune.

13 *b. Duty to disaggregate, reverse-engineer, or delete.* Where data has been processed
14 wrongfully – whether because control of the original data was wrongful (e.g. because it had been
15 obtained by way of unauthorized access, see Principle 31) or because only the processing activities
16 were wrongful (e.g. because the activities had been excluded by way of contractual limitation, see
17 Principle 30) – the controller normally must undo the processing. Where the original data has been
18 wrongfully aggregated with other data, the controller is under an obligation to disaggregate the data
19 (and, if control of the data was wrongful, subsequently give up any control of the relevant data after
20 disaggregation). Where derived data has wrongfully been obtained by way of processing the
21 original data, this basically means reverse-engineering (unless, where control was wrongful, the
22 controller can delete both the original and the derived data). The same basically holds true for
23 inferred data, which normally must be deleted if wrongfully obtained.

24 *c. Limits on duty to disaggregate.* Principle 36(2) states that disaggregation, reverse-
25 engineering, or deletion of data is not required to the extent that it is not possible or would mean a
26 destruction of values that is unreasonable in light of the circumstances giving rise to wrongfulness
27 on the part of the controller and the legitimate interests of any party protected under Chapter A.
28 Where these conditions are met, an allowance may be made in money whenever and to the extent
29 this is reasonable in the circumstances. Such an allowance may be combined with restrictions on

1 further use of the derived data. What counts as ‘unreasonable’ must be assessed in the
2 circumstances, taking into account a number of factors. The list of factors provided in paragraph
3 (2) is not exhaustive. It includes: (a) whether or not the controller had notice of the wrongfulness
4 at the time of processing; (b) whether or not wrongfulness was fundamental in the circumstances
5 or could be expected to cause relevant material harm to a party protected under Chapter A; and (c)
6 the amount of investment made in processing, and the relative contribution of the original data to
7 the derived data.

8 **Illustrations:**

9 164. In the scenario described in Illustration no. 163, a court would take into account that
10 social network provider P had notice of the wrongfulness and was acting recklessly,
11 that biometric data is extremely sensitive data and that, even if the resulting facial
12 recognition AI does not refer to a particular individual, it affects particular groups of
13 individuals in their fundamental rights, and that the purposes were purely commercial
14 in nature. In such a situation a court should not grant an exception under Principle 36(2),
15 even where P has made significant investment in the processing.

16 165. Company C wants to develop a new AI for helping combat a pandemic. For this
17 purpose, C buys ‘anonymised’ medical data from recognized medical service provider
18 M. As C does not attempt to create any link between the data and any individuals, it
19 escapes C’s attention that, with advanced technological means and after combining the
20 data with other data, an individual could theoretically be re-identified, so that the data
21 counts as ‘personal data’ within the meaning of the applicable data protection regime.
22 In this case, a court should consider that C was acting in good faith, that the
23 wrongfulness was not fundamental and there was no actual risk for data subjects, and
24 that processing occurred for an important purpose. Therefore, a court would be inclined
25 to grant an exception to the general obligation to undo the processing.

26 Where the controller is not obligated under Principle 36 to undo the processing, Principle
27 35 still applies. It requires that, if the controller faces duties and restrictions with regard to the
28 derived data, these duties and restrictions may still prevail.

1 1923172, at 2, 5 (F.T.C. Jan. 11, 2021), available at
 2 https://www.ftc.gov/system/files/documents/cases/everalbum_order.pdf. This represented a
 3 departure from prior consent orders that allowed companies to retain algorithms derived from
 4 illegally obtained data. See *In re Google LLC and YouTube, LLC*, File No. 1723083 (F.T.C. Sept.
 5 10, 2019), available at
 6 https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf.
 7 Restitution applies to conscious interference with other protected interests, including the right to
 8 privacy, assuming disgorgement is susceptible of measurement, would not be inequitable, and
 9 would not conflict with limits imposed by other law. See Restatement, Third, Restitution and
 10 Unjust Enrichment § 44 and Comment *b*. Claimants may obtain restitution from any products
 11 traceable to wrongfully obtained property. See Restatement, Third, Restitution and Unjust
 12 Enrichment § 58. Bona fide purchasers are exempt from equitable remedies. See Restatement,
 13 Third, Restitution and Unjust Enrichment § 66.

14 The right to derived data based on processing conducted before control became wrongful is likely
 15 to arise in conjunction with the consumer right to require deletion of personal data provided by
 16 some state statutes. See CAL. CIV. CODE § 1798.105; VA. CODE ANN. § 59.1-573(A)(3). In
 17 California, businesses may comply with requests for deletion by deidentifying or by aggregating
 18 the information. CAL. CODE REGS. tit. 11, § 999.313(d)(2).

19

20

Europe:

21 *a. General observations, b. Duty to disaggregate, reverse-engineer, or delete and c. Limits*
 22 *on duty to disaggregate.* The duties under Principle 36 have certain similarities with Articles 12 f.
 23 Trade Secrets Directive (Directive (EU) 2016/943). If a trade secret has been unlawfully acquired,
 24 used or disclosed, the competent judicial authorities may, at the request of the applicant, order one
 25 of the injunctions or corrective measures listed in Article 12 Trade Secrets Directive. These
 26 measures include the destruction of all or part of any document, object, material, substance or
 27 electronic file containing or embodying the trade secret. However, at the request of the person
 28 liable to be subject to measures (including erasure), the competent judicial authority may order
 29 pecuniary compensation to be paid to the injured party instead of applying those measures if all the
 30 following conditions of Article 13(3) of the Directive are met: (a) the person concerned at the time
 31 of use or disclosure neither knew nor ought, under the circumstances, to have known that the trade
 32 secret was obtained from another person who was using or disclosing the trade secret unlawfully;
 33 (b) execution of the measures in question would cause that person disproportionate harm; and (c)
 34 pecuniary compensation to the injured party appears reasonably satisfactory.

35 The considerations underlying Principle 36 have some similarities to the doctrines of
 36 combination and commingling in the tangible world (for a comparative overview see Brigitta
 37 Lurger and Wolfgang Faber, *Principles for European Law - Study on a European Civil Code -*
 38 *Acquisition and Loss of Ownership in Goods*, 2013, p. 1150 ff., 1180 ff.), even though this
 39 Principle does not follow the logic of property rights.

40 These rules also set out the primary obligation, to separate the resulting mass or mixture
 41 into its original constituents, as does Principle 36(1). In this case the initial owners simply remain
 42 owners of the respective parts and claim return based on general principles of ownership and
 43 possession. However, the consequences if it is impossible or economically unreasonable to separate
 44 the resulting mass or mixture are quite different from those provided in Principle 36(2).

1 Where goods owned by different persons are commingled and it is impossible or
2 economically unreasonable to separate the resulting mass or mixture into its original constituents,
3 but it is possible and economically reasonable to separate the mass or mixture into proportionate
4 quantities, these persons become co-owners of the resulting mass or mixture, each for a share
5 proportionate to the value of the respective part at the moment of commingling (Article VIII.-5:202
6 DCFR: Article VIII.-5:202 PEL Acq. Own.).

7 The rules on combination under Article VIII.-5:203 DCFR and Article VIII.-5:203 PEL
8 Acq. Own. provide that in the case that one of the component parts is found to be the principal part,
9 the owner of that part normally acquires sole ownership of the whole, and the owner or owners of
10 the subordinate parts are entitled, against the sole owner, to payment secured by a proprietary
11 security interest in the combined goods. Where none of the parts is to be regarded as the principal
12 part, the owners of the component parts become co-owners of the whole, each for a share
13 proportionate to the value of the respective part at the moment of combination. If, in the case of
14 more than two component parts, one component part is of minimal importance in relation to other
15 parts, the owner of this part is entitled, against the co-owners, only to payment proportionate to the
16 value of the respective part at the moment of combination.

17 *d. Application with regard to products and services.* Paragraph (3) gives the protected
18 parties under Chapter A similar protection as under the Trade Secrets Directive which not only
19 considers the acquisition, use or disclosure of a trade secret as unlawful, but also the production,
20 offering or placing on the market of infringing goods, or the importation, export or storage of
21 infringing goods for those purposes (Article 4(5) of Directive (EU) 2016/943).

22 **Principle 37: Effect of non-material non-compliance**

23 **(1) If a controller engages in data activities with respect to a large data set, and the data**
24 **activities do not comply with duties and restrictions under Chapter A with regard to**
25 **some of the data, the law should provide that such activities are not wrongful with**
26 **regard to the whole data set if**

27 **(a) the non-compliance is not material in the circumstances, such as when the affected**
28 **data is only an insignificant portion of the data set with regard to which data**
29 **activities take place;**

30 **(b) the controller has made the efforts that could reasonably be expected in the**
31 **circumstances to comply with the duties and restrictions; and**

32 **(c) the data activities are not related to the purpose for which duties or restrictions**
33 **under Chapter A are imposed and could not reasonably be expected to cause**
34 **material harm to a protected party.**

1 **(2) When paragraph (1) applies, the controller must, upon obtaining notice, remove the**
2 **affected data from the data set for the purpose of future data activities unless this is**
3 **unreasonable in the circumstances.**

4 **Comment:** *a. General observations.* The data economy is increasingly dealing with very
5 large and diverse data sets. While the size and diversity of a data set does not in any way diminish
6 the need for protection of third parties, it is becoming more difficult for players in the data economy
7 to comply strictly with all duties and restrictions with regard to each and every data point they are
8 controlling, including data points originally collected by others. The cumulative effect of legal
9 regimes such as IP protection, data privacy/data protection, trade secret protection and contractual
10 protection may well lead to a situation in which large data sets inevitably will contain some data
11 points that are wrongful under one or another of those protective regimes. If the result of a minimal
12 amount of such non-compliance is liability or other sanctions that are disproportionate to the
13 magnitude of the non-compliance, over-deterrence may follow. For example, players in the data
14 economy might no longer risk being transparent about their activities, and no longer share their
15 data sets with others for the benefit of innovation and growth, because they are afraid that very
16 minor acts of non-compliance might lead to disproportionate reactions. This could seriously
17 endanger legitimate data activities that would ultimately be for the benefit of everyone.

18 In order to avoid such over-deterrence, Principle 37 provides that wrongfulness with respect
19 to some items in a data set should not necessarily result in treating data activities with respect to
20 the entire set as wrongful.

21 *b. Criteria for application of this rule.* Paragraph (1) of Principle 37 lists a number of criteria
22 that must all be satisfied for the rule to apply. First, the rule applies only to large data sets where
23 data activities with regard to only an insignificant amount of the data are non-compliant with duties
24 and restrictions under Chapter A. What constitutes ‘large’ will necessarily depend on the context.
25 The key element here is that the non-compliance of the data activities must affect only an
26 insignificant part of the data set, and not the whole data set.

27 **Illustration:**

28 168.Huge amounts of data from connected cars, which are being controlled by car
29 manufacturer M, qualify as personal data under the data protection law that is applicable

1 in the given case. The owners of the cars have, when first configuring their on-board
2 computers, consented to certain data processing activities, but passengers, as to whom
3 a comparatively minuscule amount of data has been collected, have not consented.
4 Assuming that, under the applicable data protection law, data activities with respect to
5 the data about the passengers is non-compliant with restrictions under Chapter A, a
6 court might consider the non-compliance as not material in the circumstances in light
7 of the fact that the data from passengers amounts to only an insignificant portion of the
8 overall data. In that case, the first criterion for application of paragraph (1) is satisfied.

9 The second criterion is the requirement under paragraph (1)(b) that the controller has made
10 efforts that could reasonably be expected in the circumstances to comply with the duties and
11 restrictions. This criterion is satisfied even if unrealistic or unreasonable measures are theoretically
12 possible.

13 **Illustration:**

14 169. In a situation such as that described in Illustration no. 168, assume that manufacturer
15 M has taken all reasonable steps that could be expected in the circumstances, including
16 both steps to ascertain what its duties and restrictions are with regard to the data, and
17 steps to avoid non-compliance. M is not required to take unrealistic or unreasonable
18 measures, such as requiring car owners to obtain consent to data processing from all
19 passengers.

20 The third criterion for application of the rule in paragraph (1) – that the type of data activity
21 engaged in by the controller is not related to the purpose for which duties or restrictions within the
22 meaning of Chapter A were imposed and could not reasonably be expected to cause harm to a
23 protected party – is important because it prevents application of the rule when the data activity in
24 question may undermine the very reason for the restrictions.

25 **Illustration:**

26 170. In a situation such as that described in Illustration no. 168, the third criterion for
27 application of the rule in paragraph (1) would not be satisfied if M's data activities were
28 for the purpose of gaining insight particularly into how often passengers are taken for a
29 ride, and how they behave with regard to the car. If, however, M's data activities were

1 for training AI with regard to how best to adjust the belt tension to a person's size, this
2 data activity is not related to the purpose for which data protection restrictions were
3 imposed, and no harm will be caused to a protected party. (Indeed, there is a possibility
4 that the improved AI will also benefit those protected parties.)

5 *c. Obligation to remove data upon request.* While application of the rule in paragraph (1)
6 protects the controller from a claim that its activities with respect to an entire data set are wrongful
7 when the controller's wrongful data activities are not material, this should not mean that the
8 controller may continue to engage in the same type of data activities with the affected data.
9 Accordingly, paragraph (2) provides that when a controller's data activities is non-compliant, the
10 controller must still remove the affected data from the data set for future processing upon request
11 by a protected party unless removal would be unreasonable in the circumstances.

12 **Illustration:**

13 171. Assume that, in a situation such as that described in Illustration no. 168, passenger P
14 learns about M using passenger data for training its belt tension AI and requests M to
15 remove P's personal data from the data set. If this can be done easily without
16 burdensome and expensive efforts, M must comply with the request.

17 *d. Relationship to other law.* This Principle is, of course, subject to contrary doctrines in
18 data protection/data privacy law, intellectual property law, etc., see Principle 1(3). Nonetheless,
19 this Principle serves important purposes. First, Chapter A addresses not only protection arising
20 from those bodies of law but also from other areas such as contract. Second, even the areas of law
21 to which these Principles defer may not fully address these issues, in which case this Principle may
22 serve as a gap filler. Third, to the extent that those areas of law evolve and develop, this Principle
23 may provide a useful source of factors to consider in that process.

24 **REPORTERS' NOTES:**

25 **U.S.:**

26 U.S. law frequently distinguishes between substantial performance of duties on one hand
27 and material breach of duties on the other hand. In the context of installment contracts, for
28 example, see UCC § 2-612. More generally, see, e.g., Restatement (Second) of Contracts § 237
29 ("... it is a condition of each party's remaining duties to render performances to be exchanged under
30 an exchange of promises that there be no uncured material failure by the other party to render any

1 such performance due at an earlier time”). A well-known case examining this concept is *Jacob &*
2 *Youngs v. Kent*, 230 N.Y. 239, 129 N.E. 889 (1921). See also *Lovink v. Guilford Mills, Inc.*, 878
3 F.2d 584, 587 (2d Cir. 1989).

4 **Europe:**

5 *a. General Observations.* If a data set covers data protected by third party rights, these third-
6 party rights typically apply to the whole set of data if it is not possible to separate the affected data.
7 For example, according to Article 2(2) Free Flow of Data Regulation (Regulation (EU) 2018/1807)
8 the GDPR shall apply where the data set contains personal data that is inextricably linked with the
9 non-personal data. The European Commission has further specified that the GDPR shall apply
10 regardless of the extent to which personal data are included in mixed datasets. Hence, the GDPR
11 applies, even if the personal data only represents a marginal share of the aggregated data
12 (COM(2019) 250 final, p. 9).

13 *b. Criteria for application of this rule and c. Obligation to remove data upon request.* In
14 contrast to the Free Flow of Data Regulation, Principle 37 set out that wrongfulness with respect
15 to some items in a data set should only result in treating data activities with respect to the whole
16 data set as wrongful, if the criteria in paragraph (1)(b) and (c) are also fulfilled. These partly overlap
17 with the criteria set forth in Principle 36, which is why reference is made to the Notes in Principle
18 36.

19 **Part V: Multi-State Issues**

20 **Principle 38: Application of established choice-of-law rules of the forum**

21 **(1) When an issue is within the territorial scope of the law of more than one State, the law**
22 **applicable to that issue is determined by the forum's choice of law rules. These Principles**
23 **do not determine the territorial scope of a State's law.**

24 **(2) The law applicable to data contracts under Part II should be the law of the State that**
25 **would be selected under the forum's choice of law rules for contracts.**

26 **(3) For any other issue arising under these Principles, the law applicable to that issue should**
27 **be**

28 **(a) the law of the State that would be selected under the forum's choice of law rules if**
29 **those rules provide a clear rule for determining the law applicable to that issue; or**

30 **(b) if the forum's choice of law rules do not provide a clear rule for determining the**
31 **law applicable to that issue, the law determined by application of Principle 39.**

1 **Comments:** *a. General observations.* The characteristics of digital data are such that there
2 are few natural barriers to cross-border data transactions. Modern forms of electronic
3 communication make it easy for the parties to such a transaction to communicate with each other,
4 and data controlled by a party in one State can easily be transferred to a party in another State or
5 be accessed by a party in another State. While legal relationships concerning data are already very
6 complex in a purely domestic setting, the analysis of rights and duties of the parties is even more
7 complex when the parties are in different States inasmuch as rights and duties may be different in
8 one State than in the other. When a matter touches more than one state, differences between the
9 law of one of the states and that of another are resolved by application of the forum's choice of law
10 rules.

11 Principle 38 should be understood as saying that courts or other authorities may continue
12 using existing, clear approaches to resolving potential choice of law issues with regard to matters
13 addressed by these Principles. It also clarifies that Part V of the Principles does not deal, in
14 particular, with how the territorial scope of a state's regulatory regimes should be defined. The
15 principles do not cover the possible interactions of regulatory regimes in a particular forum. These
16 are each issues for determination by the forum and will depend on a number of factors, which differ
17 from jurisdiction to jurisdiction, including mandatory application and the territorial extent of that
18 application.

19 *b. Deferral to the choice of law rules of the forum for contract issues.* Most States have
20 well-developed choice of law rules to determine which law governs certain relationships with an
21 international (or, in a federal system such as the U.S., an interstate) element. This holds true, in
22 particular, for contracts, including the data contracts addressed in Part II. These rules (which may
23 vary depending on whether or not the parties have agreed on what law is to govern their contract
24 and whether the contract is between businesses or whether a consumer is involved) are typically
25 general in nature and apply across a wide range of contracts. Principle 38(1) recommends that a
26 forum apply those general choice of law rules to data contracts rather than devise a special rule for
27 data transactions.

28 Choice of law rules in most States give the parties to a cross-border contract substantial
29 leeway to select the law governing their contract. In business-to-business transactions, many States
30 allow the parties to a cross-border contract to select the law of any State to govern their contract,
31 subject only to fundamental notions of public policy of the forum (or of another state whose law

1 would be applicable in the absence of a choice of law by the parties) or application of an overriding
2 mandatory provision of the forum’s law. Other States similarly allow the parties to a cross-border
3 transaction to select the State whose law will govern that contract, but limit that choice to the
4 selection of a State that bears some sort of relationship to the parties or the contract. States vary as
5 to the ability of parties to select the governing law in contracts with consumers, with some States
6 reducing the range of possible choices in some contexts.

7 **Illustration:**

8 172. Company S, established in State X, sells a large data set to company R, established in
9 State Y. S and R agree to have their contract governed by the law State X. Assume that
10 a dispute arises and is litigated in the courts of State Y. If the choice-of-law rules of
11 State Y give effect to the parties’ choice of the applicable law, the contract will be
12 governed by the law of State X.

13 When the forum’s choice of law rules are applied in a context in which the law of one or
14 more states regulates in an area of substantial public concern rather than simply allocating private
15 rights, the role of overriding mandatory provisions of the forum’s law may increase and sometimes
16 result in application of the forum’s law to a particular topic without regard to the law of other states
17 whose law might otherwise apply. In such a context of substantial public concern, where the public
18 policies of states may differ significantly, it is also possible that, when application of a forum’s
19 choice of law rule initially refers a matter to the law of another state, the law of that other state may
20 be manifestly incompatible with fundamental notions of public policy of the forum (or of another
21 state whose law would be applicable in the absence of a choice of law by the parties) and, therefore,
22 its application to the matter will be excluded.

23 *c. Deferral to choice of law rules of the forum for other issues as to which the forum state*
24 *has clear rules.* While existing choice of law rules for contracts apply directly to data contracts
25 within the meaning of Part II (as they would apply to contracts unrelated to data), the situation is a
26 bit different with other legal issues addressed by the Principles, notably with data rights under Part
27 III, and in particular rights in co-generated data. Such data rights are not yet an established area of
28 the law in most legal systems, with the possible exception of open data in the public sector.
29 Similarly, most legal systems do not have clear and well-established conflict of laws rules with
30 respect to data rights (or more general concepts that map onto data rights).

1 For states that do have such rules, or develop them in the future, by creating new paradigms
2 or integrating rules with respect to data rights into existing and well-established frameworks, such
3 as contract law, tort law, property law or competition law, this Principle recommends deferral to
4 them.

5 **Illustration:**

6 173. A court in State X is confronted with the question of whether airline A in Illustration
7 83 has a right against D to be provided with access to the data, and the law of the relevant
8 states differ so that the court must determine which state's law is applicable. If the
9 choice-of-law rules of State X provide clear rules to determine which state's law
10 governs matters addressed in Part III of these Principles, those choice-of-law rules
11 should be applied by the court to determine the applicable law.

12 174. Company S established in State X sells goods over the online marketplace run by
13 platform provider P established in State Y. A dispute arises as to whether S, which seeks
14 to move to another online marketplace run by Q, has a right against P to have S's
15 reputational data from customer reviews transferred to Q. If, according to the choice of
16 law rules of the forum, the law of State Y clearly governs matters of competition, and
17 where the law of State Y has implemented access rights in co-generated data in
18 competition law, those parts of the competition law of State Y would apply.

19 The same considerations apply to other legal issues addressed, directly or indirectly, by
20 these Principles and for which established choice of law rules exist, such as for IP protection and
21 infringements of IP rights, which are not dealt with by these Principles, but addressed as given
22 under Part IV. Similarly, where under a clear and well-established approach, the courts of the forum
23 state apply a particular regulatory regime of that state to all matters that are within the territorial
24 scope of that regulatory regime, Principle 38(2)(a) recommends that that approach should continue
25 to be followed.

26 For States that do not have choice-of-law rules that provide clear guidance for determining
27 the law applicable to an issue, Principle 39 identifies several factors to be used in choice-of-law
28 analysis.

29 **REPORTERS' NOTES:**

30 **U.S.:**

1 For U.S. choice of law principles applicable to contracts, see Restatement (Second),
2 Conflict of Laws, Chapter 8. Party autonomy to select the law governing a contract is addressed in
3 Restatement (Second), Conflict of Laws § 187. General principles that determine the applicable
4 law in the absence of an effective choice by the parties are addressed in Restatement (Second),
5 Conflict of Laws § 188. See also Restatement (Third), Conflict of Laws, Preliminary Draft No. 6,
6 §§ 8.01-8.02 (September 29, 2020).

7 The Hague Principles on Choice of Law in International Commercial Contracts (‘HCCH
8 Principles’) apply, where the contract is international and where the parties act in the exercise of
9 their trade or profession. A contract is ‘international’ within the HCCH Principles, unless the
10 parties have their establishments in the same State and the relationship of the parties and all other
11 relevant elements, regardless of the chosen law, are connected only with that State (Article 1(2)).
12 Furthermore, each party to the contract must be acting in the exercise of its trade or profession. The
13 Principles expressly exclude from their scope certain specific categories of contract types in which
14 one party – such as a consumer or employee – is presumptively usually in weaker bargaining
15 position, e.g. consumer and employment contracts (Article 1(1)). According to the Hague
16 Principles, international contracts within the HCCH Principles are governed by the law chosen by
17 the parties (Article 2(1)). The choice of law must either be explicit or appear clearly from the
18 provisions of the contract or the circumstances (Article 4). However, the HCCH Principles do not
19 require a connection between the law chosen and the parties or their transaction (Article 2(4)). The
20 law chosen by the parties shall govern all aspects of the contract between them, including but not
21 limited to (a) interpretation; (b) rights and obligations arising from the contract; (c) performance
22 and the consequences of non-performance, including the assessment of damages; (d) the various
23 ways of extinguishing obligations, and prescription and limitation periods; (e) validity and the
24 consequences of invalidity of the contract; (f) burden of proof and legal presumptions; and (g) pre-
25 contractual obligation (Article 9). However, the HCCH Principles shall not prevent a court from
26 applying overriding mandatory provisions of the law of the forum which apply irrespective of the
27 law chosen by the parties (Article 9(1)). A court may exclude application of a provision of the law
28 chosen by the parties only if and to the extent that the result of such application would be manifestly
29 incompatible with fundamental notions of public policy (*ordre public*) of the forum (Article 9(2)).
30

31 U.S. law lacks a uniform rule governing choice of law. Most states have adopted the
32 Restatement (Second), Conflict of Laws, while others have adhered to Restatement (First), Conflict
33 of Laws, and still others have adopted a hybrid approach. Both § 6 of the Second Restatement and
34 § 7 of the First Restatement endorse the approach adopted by Principle 38, which provides that
35 courts should resolve choice-of-law issues under forum law. Courts have applied the forum’s
36 choice of law rules to contracts for data. *In re Facebook Biometric Info. Privacy Litig.*, 185 F.
37 Supp. 3d 1155, 1167-68 (N.D. Cal. 2016); *Peterson v. Martinez*, No. A17-0355, 2017 WL
38 6418224, at *4 (Minn. Ct. App. Dec. 18, 2017).
39

40 Section 187 of the Second Restatement explicitly endorsed the application of choice-of-law
41 clauses in contracts, deviating from the First Restatement’s hostility toward the practice. Even
42 states that adhere to the First Restatement approach have generally adopted a policy of favoring
43 the enforceability of choice-of-law clauses.
44

45 Section 188 of the Second Restatement lays out the principles that determine the applicable
46 law in the absence of a choice-of-law clause. The section identifies the key question of which state

1 has the most significant relationship to the transaction and the parties, and five specific types of
2 contacts that courts should take into account when making this determination.

3 **Europe:**

4 *a. General Observations.* In Europe, there are different approaches to resolving a potential
5 conflict between the laws, including any regulatory regimes, of two or several states whose law
6 might be applicable in a cross-border situation. First and foremost, there may be legal provisions
7 applicable in the forum state that directly and specifically address cross-border situations, including
8 by way of international uniform law, such as the UN Convention on the International Sale of Goods
9 (CISG). Secondly, for a number of regulatory regimes, there may be specific rules defining the
10 territorial scope of the regulatory regime. Where this is the case, a national court or other authority
11 that has assumed jurisdiction would normally not even consider the application of foreign law but
12 simply apply the regulatory regime to any situation that is within the territorial scope of that regime.
13 This method is used for a broad range of legal instruments that are commonly considered as ‘data
14 law’, including the GDPR (Regulation (EU) 2016/679), the Free Flow of Data Regulation
15 (Regulation (EU) 2018/1807), the Platform-to-Business Regulation (Regulation (EU) 2019/1150),
16 as well as the future E-Privacy Regulation (Commission Proposal COM(2017), 10 final), Data
17 Governance Act (COM(2020) 767 final), Digital Services Act (COM(2020) 825 final), Digital
18 Markets Act (COM(2020) 842 final), AI Act (COM(2021) 206 final) and most probably also the
19 future Data Act (cf. COM(2020) 66 final 13) a proposal for which is expected in late 2021. In some
20 legal instruments, such as the Open Data Directive (Directive (EU) 2019/1024, or, rather, national
21 law implementing the Directive) and much of sectoral legislation, rules on territorial scope are
22 more implicit. Thirdly, legal instruments may also explicitly or implicitly mandate the recognition
23 (or, in fact, non-recognition) of certain foreign elements, e.g. in areas where the GDPR leaves a
24 degree of leeway to the Member States and thus the requirements may differ from state to state it
25 is held that a controller engaging in cross-border data activities only needs to fulfil the requirements
26 of their own state (see Recital 153, 6th sentence, GDPR), although the matter is still disputed.
27 Fourthly, as far as a matter is governed by the more traditional areas of what is often considered to
28 be ‘private law’, such as contract and tort, but also intellectual property law or competition law,
29 the forum’s choice-of-law rules (which, in turn, may be of international, EU or domestic origin)
30 would designate the applicable law by way of connecting factors and a range of specific choice-of-
31 law methods and doctrines (such as classification, *dépeçage*, *renvoi*, assimilation or *ordre public*).
32 It is only in the context of the fourth (and, to a certain extent, the third) of the four approaches just
33 explained that a court or other authority would genuinely consider the ‘application’ of foreign law,
34 but even in this situation there are different views as to what extent the foreign law is genuinely
35 applied as law (for example in Germany, see Reinhold Geimer, *Internationales Zivilprozessrecht*,
36 7th Edition, 2015, p. 963 f and in France, see Cass. Civ. 18.9.2002, Bull. Civ. I Nr. 2) or more as
37 fact (for example in the UK, see *Bumper Development Corpn. v. Comr. of Police* [1991] 1 W.L.R.
38 1362, 1368). Only as far as Principle 38(1) states that courts or other authorities may continue using
39 existing, clear approaches to resolving potential choice of law issues it refers to all four approaches
40 just described. However, it also clarifies that Part V of the Principles does not deal, in particular,
41 with how the territorial scope of regulatory regimes should be defined (i.e. it does not give any
42 specific guidance with regard to the third approach).

43 *b. Deferral to choice of law rules of the forum.* In Europe, data contracts under Part II are
44 governed by the Rome I Regulation which lays down rules on the conflict of laws for contractual
45 obligations in civil and commercial matters (Article 1(1) of Regulation (EC) No 593/2008). A
46 contract shall generally be governed by the law chosen by the parties. The choice of law can be

1 made expressly or be clearly demonstrated by the terms of the contract or the circumstances of the
2 contract (Article 3). In Articles 5 to 8, the Regulation lays down rules for the law applicable to
3 contracts of carriage, consumer contracts, insurance contracts and individual employment
4 contracts. If the applicable law is not chosen and none of Articles 5 to 8 apply, the law governing
5 the contract shall be determined by Article 4(1) of the Regulation, which specifies the law
6 applicable to certain contracts. The list of contracts specifically mentioned includes sales contracts
7 (Article 4(1)(a)), service contracts (Article 4(1)(b)) and the sale of immovable property (Article
8 4(1)(c)). If the contract is not covered by the specific rules of Article 4(1) or if the elements of the
9 contract would be covered by more than one point, the contract is governed by the law of the
10 country where the party required to effect the characteristic performance of the contract has its
11 habitual residence (Article 4(2)). However, where it is clear from all the circumstances of the case
12 that the contract is manifestly more closely connected with a country other than one indicated in
13 Article 4(1) and (2), the law of that country shall apply instead (Article 4(3)). When the law
14 applicable to the contract can still not be determined, the contract is governed by the law of the
15 country with which it is most closely connected (Article 4(4)).

16 The Rome I Regulation follows the rule introduced by its predecessor, the Rome
17 Convention, that the contract is governed by the law of the State where the party required to effect
18 the characteristic performance of the contract has its habitual residence. For most contracts for
19 supply or sharing of data under Part II Chapter B, the characteristic performance is not the
20 remuneration paid by the recipient, but the performance by the supplier. Therefore, the rules set
21 out in Article 4(1) or (2) of the Rome I Regulation will generally lead to the application of the law
22 of the country in which the supplier has its habitual residence. This may be different for contracts
23 for authorization to access under Principle 10, as authorization to access is often provided in lieu
24 of a consideration in money, such as in many mass contracts for digital content or digital services.
25 In these cases, the characteristic performance will be the supply of the digital content or service.
26 Where such cases involve consumer contracts, the special rules under Article 6 take priority, which
27 often lead to the application of the law of the consumer's habitual residence. Contracts for data
28 pooling within the meaning of Principle 11 will often be governed by the law of the otherwise
29 closest connection according to Article 4(4), unless rules of international company law come into
30 play.

31 Contracts for services with regard to data (Part II Chapter C) would fall under the broad
32 notion of 'contracts for the provision of services' under Article 4(1)(b) of the Regulation which
33 applies to activities in return for remuneration (see CJEU, Case C-533/07 ECLI:EU:C:2009:257 –
34 *Falco Privatstiftung*). Thus, the law of the country where the service provider has its habitual
35 residence applies.

36 *c. Deferral to choice of law rules.* In Europe, the law applicable to data rights under Part III
37 is primarily determined by the choice of law rules and similar rules in existing specific legislation
38 (see Christiane Wendehorst, in Jürgen Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg,
39 *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, Band 13 – Internationales Privatrecht,
40 2020, Art. 43 EGBGB no. 297 f.). Apart from the many instances where a matter will be dealt with
41 by a regulatory regime that defines its own territorial scope (see above at a.), this will typically lead
42 to the application of the Rome I and the Rome II Regulations where data rights have been
43 implemented in a framework of contractual or non-contractual obligations.

44 The Rome II Regulation (Regulation (EC) No 864/2007) governs non-contractual
45 obligations, such as arising out of a tort/delict. As a general rule, the Regulation leads to the
46 application of the law of the country in which the damage occurs irrespective of the country in
47 which the event giving rise to the damage occurred and irrespective of the country or countries in

1 which the indirect consequences of that event occur (Article 4(1)). But where the person claimed
2 to be liable and the person sustaining damage both have their habitual residence in the same country
3 at the time when the damage occurs, the law of that country shall apply (Article 4(2)).

4 However, data rights may be implemented under competition law or intellectual property
5 law for which the Rome II Regulation provides specific rules in its Articles 6 and 8, which take
6 priority over the general rule in Article 4.

7 As to obligations arising out of acts of unfair competition, the Rome II Regulation
8 differentiates between market-related and competitor-related acts. If the act in question affects the
9 public, i.e. a ‘market related act’, Article 6(1) provides for the law of the country where the interests
10 protected by the law of unfair competition are affected. However, if the act only affects the interests
11 of a specific competitor, i.e. a ‘competitor-related act’, Article 6(2) refers to the general rule of
12 Article 4 and thus the usual rules on the law applicable to obligations arising from tort/delict apply.
13 In contrast, the law applicable to a non-contractual obligation arising out of a restriction of
14 competition is determined by the ‘market effects principle’, which leads to the application of the
15 law of the country, whose market is, or is likely to be, affected (Article 6(3)(a)).

16 European Intellectual Property Law is dominated by the *lex loci protectionis*, which is
17 stated in Article 8(1) Rome II Regulation. The law applicable to a non-contractual obligation
18 arising from an infringement of an intellectual property right is the law of the country for which
19 protection is claimed. While this is unproblematic in single-state scenarios, it leads to the
20 application of the laws of all countries for which the plaintiff claims protection, if an act of
21 infringements affects intellectual property rights in a number of countries (so called ‘mosaic
22 approach’).

23 It is important to note that the Rome II Regulation excludes certain obligations from its
24 scope, among them obligations arising of violations of privacy and rights relating to personality
25 (Article 1(2)(g) Rome II), and obligations arising from an infringement of the GDPR. Given that
26 claims for damages under the GDPR may follow slightly different rules from jurisdiction to
27 jurisdiction, it may be important to determine which law of damages applies. However, the GDPR
28 does not contain any detailed choice of law rules. This was not the case under the previous data
29 privacy regime with the Data Protection Directive (Directive 95/46/EC), which provided for
30 application of the law of the country to which the activities of the controller were directed, if the
31 controller carried out the data processing in question in the context of the activities of an
32 establishment situated in that country (Case C-191/15 ECLI:EU:C:2016:612 – *Verein für*
33 *Konsumenteninformation v Amazon EU Sàrl*). However, it is unclear to what extent this judgement
34 is still relevant in determining the applicable national law under the GDPR. It is more convincing
35 to conclude from Recital 153 GDPR, which basically refers to the law of the Member State to
36 which the controller is subject in the context of freedom of expression (see also Article 6(3)(b),
37 Article 23 GDPR), that the law of only *one* country should apply. This would mean that the GDPR,
38 at least for intra-European choice-of-law conflicts, generally follows the country-of-origin rule
39 (Marian Thon, *Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO,*
40 *2019 Rabels Zeitschrift für ausländisches und internationales Privatrecht*, p. 24, 44 f.).

41 **Principle 39: Issues not covered by established choice of law rules of the forum**

42 **(1) The law applicable to issues not already covered by Principle 38 should be the law of the**
43 **State that has the most significant relationship to the legal issue in question. Contacts to**

1 **be taken into account in determining which State has the most significant relationship**
2 **include:**

3 **(a) the place where data activities (i) are designed to produce effects on relevant**
4 **interests or (ii) actually produce effects;**

5 **(b) the domicile, residence, nationality, place of incorporation and place of business of**
6 **the party asserting a right and the party against whom it is asserted; and**

7 **(c) the law of the State that governs a pre-existing legal relationship, if any, between**
8 **the party asserting a right and the party against whom it is asserted; and**

9 **(d) the place where the data is generated.**

10 **(2) Parties may, by mutual agreement made after a dispute has arisen, choose the State**
11 **whose law will govern their legal relationship with regard to a legal issue addressed by**
12 **these Principles, unless this is incompatible with the nature of the legal issue or**
13 **considerations of public policy.**

14 **Comments:** *a. General observations.* While conflict of laws issues with respect to contract
15 matters are covered by Principle 38(2) and conflict of laws issues with respect to other issues may
16 be covered by Principle 38(3), there may be legal issues relating to data with regard to which the
17 forum State does not provide clear established choice of law rules. Principle 39 provides guidance
18 as to the factors to be taken into account in making conflict of laws decisions for those issues.

19 *b. Most significant relationship.* Where the law applicable to an issue related to data is not
20 determined by application of the choice of law rules referred to in Principle 38, Principle 39
21 recommends that the legal issue be governed by the law of the State that has the most significant
22 relationship to that issue. Paragraph (1) of this Principle lists four categories of contacts to be taken
23 into account in determining which State has the most significant connection to the issue. Each of
24 those categories is worthy of consideration in a choice of law determination.

25 First, it is appropriate to consider the place where data activities are designed to produce
26 effects, or where they actually produce effects. The second connecting factor relates to the location
27 of the parties, inasmuch as the States in which they are located have an obvious interest in
28 application of their legal rules.

1 **Illustration:**

2 175.A drives a connected car in Austria, his home State. He bought the car from retailer B
3 in Germany. The data collected by the connected car is controlled by U.S. manufacturer
4 M. For purposed of maintenance for the car, A seeks access to the data under Principle
5 20. When determining the law applicable to any access right A may have against M, the
6 court should consider that the data has been generated in Austria, that data processing
7 has serious effects on maintenance to be carried out in Austria, and that the residence
8 of A is in Austria, while M’s place of business is in the U.S.

9 Thirdly, paragraph (1)(d) provides that the law governing a pre-existing legal relationship
10 should be taken into account when assessing the State that has the most significant relationship
11 with the data right at issue.

12 **Illustration:**

13 176.When A and M in Illustration no. 175 have some form of relationship, for example,
14 stemming from an end user licence contract, the law applicable to this relationship
15 should also play a role when determining the most significant relationship of the data
16 right asserted by A against M. However, the sales contract with B should not be
17 considered because it is a legal relationship with a different party.

18 Last but not least, and particularly with regard to data rights that arise of out the generation
19 of data (i.e. rights in co-generated data under Chapter B of Part II), it is appropriate that a
20 connecting factor be the place or places in which the data was generated, which is typically the
21 place at which the activity that led to the generation of the data took place.

22 *c. Choice of applicable law by the parties.* Paragraph (2) permits the parties to choose, by
23 mutual agreement made after a dispute has arisen, the State whose law will govern their legal
24 relationship with regard to a legal issue addressed by these Principles, unless this is incompatible
25 with the nature of the legal issue or considerations of public policy. After the litigation begins, the
26 parties should have the ability to enter into contracts that simplify resolution of their dispute and
27 make outcomes more predictable. Also, the opportunity to try the case under an agreed law allows
28 a court to clarify the disputed issues more expeditiously.

1

REPORTERS' NOTES:

2

U.S.:

3

With respect to choice of law, compare the general U.S. policy regarding choice of law, in which the factors relevant to the choice of applicable law include (a) the needs of the interstate and international systems, (b) the relevant policies of the forum, (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue, (d) the protection of justified expectations, (e) the basic policies underlying the particular field of law, (f) certainty, predictability and uniformity of result, and (g) ease in the determination and application of the law to be applied. Restatement (Second), Conflict of Laws § 6.

10

The problems addressed in the Principle are analogous to those addressed in Restatement of the Law (Second), Conflict of Laws, Chapter 9, Topic 3 (Movables).

12

Paragraph (1) is similar to the general principle laid out in Restatement of the Law (Second), Conflict of Laws § 222, which provides that choice of law turns on which state “has the most significant relationship to the thing and the parties.”

15

Courts have relied on factors similar to those in Paragraph (1) when finding sufficient contacts with a state to justify permitting out-of-state plaintiffs to assert data rights created by that state’s statutes. In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 486 (D. Minn. 2015).

19

Paragraph (2) recognizes that parties may enter into choice-of-law agreements with respect to data rights. Such choice-of-law clauses are limited by Restatement of the Law (Second), Conflict of Laws, § 187(2), which supports enforcement of such clauses unless (a) “the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties’ choice” or (b) “application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue.” Applying these principles, courts have overridden choice-of-law clauses when enforcing the choice-of-law clause would be contrary to another state’s fundamental policy and the other state has a greater interest in the outcome of the dispute. In re Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1168-70 (N.D. Cal. 2016). As for choice of law clauses entered into after a dispute has arisen, see. e.g., American Law Institute, Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes § 302 (“...the parties may agree at any time, including after a dispute arises, to designate a law that will govern all or part of their dispute.”).

33

Europe:

34

a. General observations. See Notes to ‘General observations’ on Principle 38. In particular, it is important to stress that Principle 39 only applies insofar as the forum takes a ‘connecting factor approach’ to resolving a potential conflict of laws, but does not give any guidance with regard to the territorial scope of a regulatory regime.

38

b. Most significant relationship. The ‘closest connection’ is a guiding Principle in European private international law and stated, e.g., in Article 4(4) Rome I Regulation (Regulation (EC) No 593/2008: ‘Where the law applicable cannot be determined pursuant to [Articles 4(1) and (2)], the contract shall be governed by the law of the country with which it is most closely connected’) and Article 4(3) of the Rome II Regulation (Regulation (EC) No 864/2007: ‘Where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than that indicated in Articles 4(1) or (2), the law of that other country shall apply.

44

1 A manifestly closer connection with another country might be based in particular on a pre-existing
2 relationship between the parties, such as a contract, that is closely connected with the tort/delict in
3 question.’).

4 *c. Choice of law by agreement.* Parties to non-contractual obligations are generally free to
5 submit their legal relationship to the law of their choice by an agreement entered into after the event
6 giving rise to the damage occurred, or where all the parties are pursuing a commercial activity, also
7 by an agreement freely negotiated before the event giving rise to the damage occurred (Article 14
8 (1) Rome II Regulation). However, with regard to infringements of intellectual property rights or
9 non-contractual obligations arising out of an act of unfair competition, parties may not deviate from
10 the rules on international private law (see Article 6(4) and 8(3) Rome II Regulation).

11 **Principle 40: Relevance of storage location**

12 **(1) Except as provided in paragraph (2), for choice-of-law purposes the location of the**
13 **storage of data is relevant as a connecting factor only when the issue in question relates**
14 **to storage or to rights in the medium.**

15 **(2) The location of storage of data may be relevant for choice-of-law purposes as a**
16 **connecting factor of a residual nature, such as in the absence of other connecting factors**
17 **or when consideration of other connecting factors is indeterminate.**

18 **(3) The fact that data is stored outside a State does not of itself ordinarily raise issues of**
19 **extraterritorial exercise of jurisdiction or application of law as long as there are**
20 **sufficient links between the State and the activities with respect to the data it seeks to**
21 **regulate or the entitlements with respect to the data it seeks to enforce.**

22 **Comments:** *a. The limited role of territorial location of data storage and of physical*
23 *establishment.* Data can move across the globe within fractions of a second; different parts of files
24 and other meaningful units of data may be stored in different territories; and data may be accessed
25 and processed remotely from all parts of the world. All of this results in disconnection between the
26 territorial location of data storage and any link to meaningful activities carried out with regard to
27 data and the impact of those activities. While providing a comprehensive set of choice-of-law
28 principles or principles concerning territorial reach of jurisdiction and substantive law rules for
29 legal relationships involving data is beyond the scope of these Principles, this Principle provides
30 that the territorial location of data storage is normally not relevant.

1 *b. Choice of law.* Where the law of more than one State might be applied to a particular
2 issue, courts must decide which State's law to apply. In many instances, in particular with regard
3 to contractual obligations, a choice of the applicable law made by the parties themselves will be
4 given effect by the courts. In many cases, however, the parties have not made a choice, or the issue
5 at hand is of such a nature as to prevent courts from giving effect to a choice by the parties. In that
6 case, choice of law rules and doctrines typically look to the law of the State with the most
7 significant contacts with the matter. This Principle makes clear that the location of storage of data
8 is ordinarily not a significant contact with respect to an issue unrelated to that storage.

9 **Illustration:**

10 177. Company G established in State 1 has customer data stored in cloud space provided by
11 F. F is established in State 2, but operates servers in States 3 and 4. Hacker H, who
12 operates from State 5, manages to gain access to the data stored on the servers. In
13 determining the law governing G's claim against F and/or H for damages the location
14 of the servers in States 3 and 4 should not be considered as a significant contact.

15 Exceptionally, the location of data storage may be relevant to choice of law where the rights
16 and remedies in question have a specific link with storage as such or with the rights in the medium.

17 **Illustration:**

18 178. Same situation as in Illustration no. 177, but F now takes recourse against the local
19 provider of the server in State 4. This dispute is related to storage as such; therefore the
20 fact that the servers are located in State 4 is relevant for determining the applicable law.

21 *c. Storage location as connecting factor of residual nature.* While ordinarily the location of
22 storage is not a relevant connecting factor except when the issue in question has a specific link to
23 storage or to the rights in the medium, courts may treat the location of storage as relevant when the
24 weight of other connecting factors is so similar as to make a determination of which law to apply
25 very difficult. In such a case, the territorial location of data storage may have some very limited
26 significance of a more residual nature, such as where a court has to determine the closest connection
27 and there might, but for the factor of location of storage, be an indeterminate situation.

1

U.S.

2 The relevance of the data storage location is underscored by a U.S. program created in the
3 aftermath of the 9/11 attacks to track and review transactions transmitted by individuals suspected
4 to have ties to Al Qaeda through the Society for Worldwide Interbank Financial
5 Telecommunication (“SWIFT”), which operated redundant data centers in the U.S. and the
6 Netherlands. Public disclosure of this program in 2006 led to concerns about whether U.S.
7 authorities’ ability to access European banking data violated European law. The U.S. and the EU
8 negotiated an agreement to store European data exclusively in the Netherlands effective on August
9 1, 2020. Terrorist Finance Tracking Program (TFTP), U.S. Dep’t of the Treasury,
10 [http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Fiance-
11 Tracking/Pages/tftp.aspx](http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx).

12 The issues are also presented clearly by the high-profile dispute over whether a warrant
13 obtained by the federal government under the Stored Communications Act (“SCA”) required
14 Microsoft to produce email stored in Ireland. The trial court held that the location of the requested
15 data is irrelevant so long as the party subject to the warrant has control over the requested material
16 and that requiring production of data stored aboard would not constitute impermissible
17 extraterritorial application of U.S. law. In re Warrant to Search a Certain E-mail Account
18 Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014). The Second
19 Circuit rejected all of these legal conclusions on appeal, holding that the statute lacked a clear
20 signal that Congress intended the statute to apply extraterritorially and that requiring production of
21 the email would be outside the SCA’s focus on protecting users’ privacy interest in stored
22 communications. In re Warrant to Search a Certain E-mail Account Controlled and Maintained by
23 Microsoft Corp., 829 F.3d 197 (2d Cir. 2016). The Supreme Court granted certiorari and heard oral
24 argument on the case before it was mooted by the enactment of the CLOUD Act, which expedited
25 procedures for international localization of U.S. search warrants. United States v. Microsoft, 138
26 S. Ct. 1186 (2018). Although this case turned more on the substantive provisions of the SCA than
27 on choice of law, it provides an apt illustration of the issues that can arise and the considerations
28 that are at play.

29 Although Restatement (Second), Conflict of Laws, § 6 lays out the general factors relevant
30 to the choice of applicable law, §§ 188 and 244 recognize that these factors vary somewhat in
31 importance with respect to contracts and property, respectively. Both provide that, in the absence
32 of more specific governing provisions, courts should apply the law of the state that has the most
33 significant relationship to the subject matter and the parties, and list the current location of the
34 subject matter as only one of several considerations that courts should take into account.

35 In terms of substantive law, the scope of U.S. federal statutes such as the Health Insurance
36 Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the
37 Gramm-Leach-Bliley Act (GLBA), turns on the nature of the entity, not the location of the data.
38 U.S. state privacy statutes typically apply to the data regarding residents of that state regardless of
39 where the data is stored. See, e.g., Cal. Civ. Code § 1798.140(g).

40 Regarding choice of law, some courts have included the location of computer servers as
41 one of the considerations justifying the application of a particular state’s law to a dispute. In re
42 Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 486 (D. Minn. 2015).

43

Europe:

44 As data can be moved across the globe within fractions of a second, the Principles limit the
45 relevance of the storage location of data for choice-of-law purposes. Again, it is of utmost

1 importance to stress that the Principles primarily address situations where the forum takes a
2 ‘connecting factor approach’ to resolving a potential conflict of laws and do not give any guidance
3 as to how to define territorial scope, see Notes to ‘General observations’ on Principle 38. This
4 means that also Principle 40 does not deal directly with the many instances where a conflict is
5 resolved by rules defining the territorial scope of a regulatory regime, even though the spirit of
6 Principle 40, i.e. that the location of data storage should normally not count, or count only in
7 exceptional cases, will also be relevant when it comes to the territorial scope of regulatory regimes.

8 Where data is the subject of contractual agreement, territorial location of data is irrelevant
9 under existing EU Law. Article 4(2) Rome I (Regulation (EC) No 593/2008) establishes the general
10 rule that, in the absence of an agreement, a contract shall be governed by the law of the country
11 where the party required to effect the characteristic performance of the contract has its habitual
12 residence. This is also true for sales and service contracts, which are specifically mentioned in
13 Article 4(1)(a)(b) (for more detailed elaborations, see Reporters’ Notes to Principle 38). The
14 location of the subject of the contract is only relevant only if a contract relates to a right in rem in
15 immovable property or to a tenancy of immovable property

16 Whether the storage location of data is irrelevant when damage or loss of data results from
17 a tortious act is still unclear. According to Article 4(1) Rome II Regulation (Regulation (EC)
18 No 593/2008) the applicable law to non-contractual obligations arising out of a tort/delict is the
19 law of the country where the damage occurs. Prima facie, this would indicate that the server
20 location of the damaged data determines the applicable law. However, the CJEU decision
21 *Wintersteiger* (Case C-523/10, ECLI:EU:C:2012:220) can be used as an argument that the sever
22 location should not be considered a relevant factor for determining the applicable law. The subject
23 matter of the decision was the jurisdiction in the case of a trademark infringement on the internet
24 through the use of a keyword identical to the protected trademark on a search engine. According
25 to Article 7(2) Brussels Ia (Regulation 1215/2012) the defendant may be sued both at the place
26 where the damage occurred and the place of the event giving rise to it. Regarding the latter, the
27 CJEU stated that the technical display process by the advertiser is activated, ultimately, on a server
28 belonging to the operator of the search engine. However, in view of the objective of foreseeability,
29 which the rules on jurisdiction must pursue, the place of establishment of that server cannot, by
30 reason of its uncertain location, be considered to be the place where the event giving rise to the
31 damage. Some authors argue that this approach should also apply to Rome II and suggest that cases,
32 where data is damaged or lost, should be solved by applying the ‘closest connection’ rule of Article
33 4(3) Rome II (see Carl Friedrich Nordmeier, *Cloud Computing und Internationales Privatrecht*,
34 (2010) *MultiMedia und Recht*, p. 151, 154; Georg Haibach, *Cloud Computing and European Union*
35 *Private International Law*, (2015) *Journal of Private International Law*, 252, 264ff).

36 Currently, no ownership-like rights for data exist in the EU, not even in European legal
37 systems that adhere to the ‘broad notion of legal object’. Hence, the application of the *lex rei sitae*
38 to data rights is not decisive and the storage location does not play a role for the applicable law. In
39 addition, referring to a single applicable legal system – as the *lex rei sitae* does for property rights
40 – would not be appropriate for data rights, as they are not exclusive rights, but rights that take into
41 account the special characteristic of data as a non-rivalrous good. It has been suggested to follow
42 the regime of GDPR (Article 3 and Recital 153 GDPR; see Reporters’ Notes to Principle 38) for
43 data rights that have no connection to a contractual relationship. An entity should be able to rely
44 on a data right existing in a country if the data processing in question is carried out as part of the
45 activities of an establishment of the respondent in that country. Whether the processing takes place
46 in that country or if the data are collected and processed in the context of an activity directed
47 towards that country should be considered irrelevant. (see Christiane Wendehorst, in Jürgen

- 1 Säcker/Roland Rixecker/Hartmut Oetker/Bettina Limperg, Münchener Kommentar zum
- 2 Bürgerlichen Gesetzbuch, Band 13 – Internationales Privatrecht, 2020, Art. 43 EGBGB para 296
- 3 ff).
- 4

1
2 **BLACKLETTER OF ELI FINAL COUNCIL DRAFT**

Part I: General Provisions

Principle 1: Purpose of these Principles

- 3 **(1) The Principles for a Data Economy are intended for use in legal systems in Europe, the**
4 **United States, and elsewhere. They are designed to**
- 5 **(a) bring coherence to, and move toward harmonization of, existing law and legal**
6 **concepts relevant for the data economy;**
- 7 **(b) be used as a source to inspire and guide the further development of the law by**
8 **courts and legislators worldwide;**
- 9 **(c) inform the development of best practices and guide the development of emerging**
10 **standards, including standards or trade codes that are specific to a particular**
11 **industry or industry sector;**
- 12 **(d) facilitate the drafting of model agreements or provisions to be used on a voluntary**
13 **basis by parties in the data economy;**
- 14 **(e) govern contracts or complement the law that governs them to the extent that they**
15 **provide default rules or that parties to a transaction have incorporated them into**
16 **their contract or have otherwise designated them to govern; and**
- 17 **(f) guide the deliberations of tribunals in arbitration and other dispute resolution**
18 **forums.**
- 19 **(2) These Principles recommend a legal framework that is intended to work with any form**
20 **of data privacy or data protection law, intellectual property law, or trade secrets law.**
21 **These Principles are not intended to amend or create any such law, but they may inform**
22 **the development of such other law. In the event of any inconsistency between these**
23 **Principles and such other law that cannot be overcome by interpretation, the other law**
24 **should prevail.**

Principle 2: Scope of these Principles

- 1 **(1) The primary focus of the Principles is on records of large quantities of information as**
2 **an asset, resource or tradeable commodity. The Principles do not address functional**
3 **data, i.e. data the main purpose of which is to deliver particular functionalities (such as**
4 **a computer program), and representative data, i.e. data the main purpose of which is to**
5 **represent other assets or value (such as crypto-assets).**
- 6 **(2) Subject to paragraph 3, these Principles address**
- 7 **(a) data contracts,**
- 8 **(b) data rights, and**
- 9 **(c) third party aspects of points (a) and (b).**
- 10 **(3) These Principles are not designed to apply to public bodies insofar as such bodies are**
11 **engaging in the exercise of sovereign powers.**

Principle 3: Definitions

- 12 **(1) For the purposes of these Principles the following definitions shall apply:**
- 13 **(a) ‘Data’ means information recorded in any machine-readable format suitable for**
14 **automated processing, stored in any medium or as it is being transmitted;**
- 15 **(b) ‘Copy’ means any physical manifestation of data in any form or medium;**
- 16 **(c) ‘Processing data’ means any operation or set of operations that is performed on**
17 **data, whether or not by automated means; it includes, inter alia, the structuring,**
18 **alteration, storage, retrieval, transmission, combination, aggregation or erasure of**
19 **data;**
- 20 **(d) ‘Access to data’ means being in a position to read the data and utilize it, with or**
21 **without having control of that data;**
- 22 **(e) ‘Control of data’ means being in a position to access the data and determine the**
23 **purposes and means of its processing;**

- 1 (f) ‘Controller’ means the person that, alone or jointly with other persons, has control
2 of data;
- 3 (g) ‘Processor’ means a person that, without being a controller, processes data on a
4 controller’s behalf;
- 5 (h) ‘Co-generated data’ means data to the generation of which a person other than the
6 controller has contributed, such as by being the subject of the information or the
7 owner or operator of that subject, by pursuing a data-generating activity or
8 owning or operating a data-generating device, or by producing or developing a
9 data-generating product or service;
- 10 (i) ‘Derived data’ means data generated by processing other data and includes
11 aggregated data and data inferred from other data with the help of external
12 decision rules;
- 13 (j) ‘Data contract’ means a contract the subject of which is data;
- 14 (k) ‘Data right’ means a right against a controller of data that is specific to the nature
15 of data and that arises from the way the data is generated, or from the law for
16 reasons of public interest;
- 17 (l) ‘Data activities’ means activities by a person with respect to data, such as
18 collection, acquisition, control, processing and other activities including onward
19 supply of data;
- 20 (m) ‘Supply’ of data means providing access to data to another person or putting
21 another person in control of data;
- 22 (n) ‘Supplier’ of data means a party who supplies data to another party, or
23 undertakes to do so;
- 24 (o) ‘Recipient’ of data means a party to whom data is supplied, or to be supplied;
- 25 (p) ‘Transfer’ of data means supply of data by way of which the supplier puts the
26 recipient in control of the data, whether or not the supplier retains control of the
27 data;
- 28 (q) ‘Porting’ data means initiating the transfer of data controlled by another party to
29 oneself or to a designated third party;

- 1 **(r) ‘Erasure of data’ means taking steps to assure, as far as is reasonably possible,**
2 **that the data is permanently inaccessible or otherwise unreadable; and**
- 3 **(s) ‘Notice’ means having knowledge of a fact or, from all the facts and circumstances**
4 **of which a person has knowledge, being in a position that the person can**
5 **reasonably be expected to have known of the fact.**
- 6 **(2) The terms ‘contract for the transfer of data’, ‘contract for simple access to data,**
7 **‘contract for exploitation of a data source’, ‘contract for authorization to access’,**
8 **‘contract for data pooling’, ‘contract for the processing of data’, ‘data trust contract’,**
9 **‘data escrow contract’ and ‘data marketplace contract’, and any terms denoting the**
10 **parties to such contracts, have the meanings given to them in Principles 7 to 15.**
- 11 **(3) References to a ‘person’ include natural and legal persons, private or public. References**
12 **to an ‘operation’ or ‘activity’ shall include operations or activities carried out with the**
13 **help of other persons or of machines, including any artificial intelligence.**

Principle 4: Remedies

- 14 **(1) Remedies with respect to data contracts and data rights, including with respect to any**
15 **protection of third parties in the context of data activities, should generally be**
16 **determined by the applicable law.**
- 17 **(2) Where these Principles or applicable law would mandate the return or surrender of data**
18 **by a party (the defendant) to another person (the claimant), the defendant should be**
19 **able to satisfy the obligation to return or surrender the data by, instead, erasing all of**
20 **the defendant’s copies of the data. If the claimant does not have a copy of the data, the**
21 **defendant must put the claimant in control of the data before erasing it.**

Part II: Data Contracts

Chapter A: Rules and Principles Governing Data Contracts

Principle 5: Application of these Principles to data contracts

- 1 **Data contracts under Part II should be governed, in the following order of priority, by:**
- 2 **(a) rules of law that cannot be derogated from by agreement;**
- 3 **(b) the agreement of the parties;**
- 4 **(c) any rules of the law other than those referred to in paragraph (a) that have been**
5 **developed for application to data transactions of the relevant kind;**
- 6 **(d) the terms included in the contracts by operation of Principles 7 to 15;**
- 7 **(e) application by analogy of default rules and principles of law that are not directly**
8 **applicable to data transactions of the relevant kind but that would govern**
9 **analogous transactions; and**
- 10 **(f) general principles of law.**

Principle 6: Interpretation and application of contract law

- 11 **In interpreting and applying rules and principles of contract law, the following factors,**
12 **among others, should be considered:**
- 13 **(a) the fact that data is a combination of (i) physical manifestations on a medium or in**
14 **a state of being transmitted, and (ii) information recorded;**
- 15 **(b) the nature of data as a resource of which there may be multiple copies and which**
16 **can be used in parallel by various parties for a multitude of different purposes;**
- 17 **(c) the fact that data is usually derived from other data, and that the original data set**
18 **and a multitude of derived data sets that resemble the original data set to a greater**
19 **or lesser extent may co-exist;**

- 1 (d) the fact that, while the physical location of data storage may change quickly and
2 easily, data is normally utilized by way of remote access and the physical location
3 of data storage is typically of little importance; and
4 (e) the high significance of cumulative effects and effects of scale.

Chapter B: Contracts for Supply or Sharing of Data

Principle 7: Contracts for the transfer of data

5 (1) A contract for the transfer of data is a transaction under which the supplier undertakes
6 to put the recipient in control of particular data by transferring the data to a medium
7 within the recipient's control or by delivering to the recipient a medium on which the
8 data is stored.

9 (2) Subject to agreement of the parties and to rules that take priority pursuant to Principle
10 5, the law should provide that the following terms are included in a contract for the
11 transfer of data:

12 (a) With regard to the manner in which the supplier is to perform its undertaking
13 described in paragraph (1), the data is to be transmitted electronically to a
14 medium indicated by the recipient, or provided in a way enabling the recipient to
15 port the data to a medium of the recipient's choice, unless either that mode of
16 delivery or the medium indicated is unreasonable in the light of data security
17 concerns in which case the supplier should promptly notify the recipient of those
18 concerns so that the recipient may indicate a substitute mode of delivery or
19 medium.

20 (b) With regard to the characteristics of the data supplied, including with regard to
21 nature, quantity, accuracy, currentness, integrity, granularity, and formats, as
22 well as with regard to the inclusion of metadata, domain tables and other
23 specifications required for data utilization, and to frequency of supply and any
24 updates:

- 1 **(i) The supplied data must conform to any material descriptions or representations**
2 **concerning the data made or adopted by the supplier, and to any samples or**
3 **models provided;**
- 4 **(ii) If the supplier has notice of the recipient’s particular purpose for obtaining the**
5 **data and that the recipient is relying on the supplier’s skill or judgment in**
6 **selecting the supplied data, the supplied data must be fit for the recipient’s**
7 **particular purpose; and**
- 8 **(iii) If the supplier is in the business of supplying data of the sort that is the subject**
9 **of the contract or otherwise holds itself out as having expertise with respect to**
10 **data of that sort, the supplied data must be of a quality that would reasonably**
11 **be expected in a transaction of the relevant kind.**
- 12 **(c) With regard to the control of, and other data activities with regard to, the supplied**
13 **data:**
- 14 **(i) If the supplied data is protected by intellectual property law or a similar regime,**
15 **the supplier must place the recipient in the position of having a legal right,**
16 **effective against third parties, that is sufficient to result in the recipient’s control**
17 **of the data and the right to engage in such other data activities that the**
18 **controller had notice that the recipient could reasonably expect to engage in. If**
19 **putting the recipient in that position requires additional steps to be taken by the**
20 **supplier, such as execution or recordation of a required document, the supplier**
21 **must take those additional steps;**
- 22 **(ii) The supplier must place the recipient in a position, at the time the data is**
23 **supplied, of being able rightfully to exercise control over the data and rightfully**
24 **to engage in other data activities which the controller had notice that the**
25 **recipient could reasonably expect to engage in; if, after the data has been**
26 **supplied, the recipient’s control of the data or other data activities become**
27 **wrongful this does not of itself give rise to a claim by the recipient against the**
28 **supplier;**
- 29 **(iii) The supplier must co-operate, to the extent reasonably necessary, in actions that**
30 **may be required to comply with legal requirements with respect to control of**

1 the data or other data activities which the controller had notice that the
2 recipient could reasonably expect to engage in. In addition, the supplier must
3 provide to the recipient information about any legal requirements with respect
4 to any such data activities of which the supplier has notice and of which the
5 recipient cannot be expected to be aware;

6 (iv) The recipient may utilize the data and any derived data, including by onward
7 supply to others, for any lawful purpose and in any way that does not infringe
8 the rights of the supplier or third parties, and that does not violate any
9 obligations the supplier has vis-à-vis third parties provided the recipient had
10 notice of these obligations at the time the contract for the transfer of data was
11 concluded;

12 (v) As between the parties, new intellectual property rights or similar rights created
13 by the recipient with the use of the supplied data belong to the recipient; and

14 (vi) The supplier may retain a copy of the data and may continue using the data,
15 including by supplying it to third parties.

16 (3) In determining which rules and principles should apply by way of analogy to contracts
17 for the transfer of data, as provided in Principle 5, factors to be taken into account
18 should include, among others:

19 (a) whether the contract provides for the recipient to be in control of the data for an
20 unlimited period of time or for a limited period of time; and

21 (b) whether the contract is for a single supply of data, repeated supply, or continuous
22 supply over a period of time.

Principle 8: Contracts for simple access to data

23 (1) A contract for simple access to data is one under which the supplier undertakes to
24 provide to the recipient access to particular data on a medium within the supplier's
25 control and which is not a contract for the transfer of data under Principle 7. This
26 includes contracts where the supplier, in addition to enabling the recipient to read the

1 **data, undertakes to put the recipient in a position to process the data on the medium**
2 **within the supplier’s control, or port data.**

3 **(2) Subject to agreement of the parties and to rules that take priority under Principle 5, the**
4 **law should provide that the following terms are included in a contract for simple access**
5 **to data:**

6 **(a) With regard to the mode of the recipient’s access to the data:**

7 **(i) The supplier must provide the recipient with the necessary access credentials**
8 **and remove any technical barriers to access whose removal could reasonably be**
9 **expected in a transaction of the relevant kind;**

10 **(ii) The supplier must make the data accessible in a structured and machine-**
11 **readable format of a sort that can reasonably be expected in a transaction of the**
12 **relevant kind;**

13 **(iii) The supplier must enable the data to be accessed remotely by the recipient**
14 **unless this is unreasonable in the light of data security concerns;**

15 **(iv) The recipient may process the data to which the recipient is given access only**
16 **for purposes consistent with any purposes agreed in the contract;**

17 **(v) The recipient may port data to which it is given access in the contract only when**
18 **the porting of such data can reasonably be expected in a transaction of the**
19 **relevant kind and may port data derived from the recipient’s processing**
20 **activities carried out in accordance with the contract (e.g, data derived from**
21 **data analytics); and**

22 **(vi) The recipient may read the data, process or port the data, as applicable, by any**
23 **means, including automated means, and may do so as often as the recipient**
24 **wishes during the access period agreed.**

25 **(b) With regard to the characteristics of the data to which access is provided, the**
26 **terms listed in Principle 7(2)(b) for contracts for transfer of data also apply in a**
27 **contract for simple access to data.**

1 (c) With regard to the control of any data ported by the recipient in accordance with
2 the contract, and other data activities, the terms listed in Principle 7(2)(c) for
3 contracts for transfer of data also apply in a contract for simple access to data.

4 (3) In determining which rules and principles to apply by way of analogy, as provided in
5 Principle 5, to contracts for simple access to data, consideration should be given in
6 particular to the degree to which the recipient may only view the data, may process data
7 on the medium within the supplier's control, or may port data.

Principle 9: Contracts for exploitation of a data source

8 (1) A contract for exploitation of a data source is one under which the supplier undertakes
9 to provide to the recipient access to data by providing access to a particular device or
10 facility by which data is collected or otherwise generated (the 'data source') enabling
11 the recipient to read the data, process or port data from the data source.

12 (2) Subject to agreement of the parties and to rules that take priority under Principle 5, the
13 law should provide that the following terms in addition to those provided in Principle 8
14 are included in a contract for exploitation of a data source:

15 (a) With regard to the mode of the recipient's access to the data on the data source:

16 (i) The recipient may port all data collected or generated by the data source; and

17 (ii) Access to the data is provided in real time as the data is collected or generated
18 by the data source.

19 (b) With regard to the characteristics of the data, there is no requirement that the
20 recipient will receive data of a particular quality or quantity.

21 (3) In determining which rules and principles to apply by way of analogy, as provided in
22 Principle 5, to contracts for exploitation of a data source, consideration should be given
23 in particular to:

24 (a) the degree and duration of control which the recipient is to receive over the data
25 source; and

26 (b) whether, and the degree to which, the recipient may port data.

Principle 10: Contracts for authorization to access

1 (1) A contract for authorization to access data is one under which the supplier (referred to
2 in this Principle as the ‘authorizing party’) authorizes the access to data or a data source
3 by the recipient, including usually processing or porting of the data, but where, in the
4 light of the passive nature of the authorizing party’s anticipated conduct under the
5 contract and the authorizing party’s lack of meaningful influence on the transaction, the
6 authorizing party cannot reasonably be expected to undertake any responsibilities of the
7 sort described in Principles 7 to 9.

8 (2) Subject to agreement of the parties and to rules that take priority under Principle 5, the
9 law should provide that in a contract for authorization to access:

10 (a) With regard to the mode of the recipient’s access, a term that the authorizing
11 party will facilitate or assist the recipient in gaining access is not included, and the
12 authorizing party may continue using the data or data source in any way, even if
13 this impairs the recipient’s access or even renders it impossible;

14 (b) With regard to the characteristics of the data, there is no requirement that the
15 recipient will receive data of a particular quality or quantity;

16 (c) With regard to control of the data and any other data activities the recipient may
17 engage in, the authorizing party has no obligation to ensure that the recipient will
18 have any particular rights;

19 (d) As between the authorizing party and the recipient, the recipient is responsible for
20 compliance with any duties vis-à-vis third parties under Part IV, including the
21 duties incumbent on a supplier of data under Principle 32; and

22 (e) The recipient must indemnify the authorizing party for any liability vis-à-vis third
23 parties that follows from the authorizing party’s authorization to access the data
24 unless such liability could not reasonably be foreseen by the recipient.

25 (3) In determining which rules and principles to apply by way of analogy, as provided in
26 Principle 5, to contracts for authorization to access data, consideration should be given
27 to whether the focus of the agreement between the parties is on the access to the data or

1 **on the supply of another commodity (such as a digital service) in the course of which**
2 **access to the data occurs.**

Principle 11: Contracts for data pooling

3 **(1) A contract for data pooling is one under which two or more parties (the ‘data partners’)**
4 **undertake to share data in a data pool by**

5 **(a) transferring particular data to a medium that is jointly controlled by the data**
6 **partners or that is controlled by a data trustee or escrowee or other third party**
7 **acting on behalf of the data partners; or**

8 **(b) granting each other access to particular data or the possibility to exploit particular**
9 **data sources, with or without the involvement of a third party.**

10 **(2) This Principle applies, with appropriate adjustments, to the governing principles of any**
11 **entity created pursuant to a data pooling contract.**

12 **(3) Subject to agreement of the parties and to rules that take priority pursuant to Principle**
13 **5, the law should provide that the following terms are included in a contract for data**
14 **pooling:**

15 **(a) A data partner may utilize data from the data pool, or data derived from such**
16 **data, only**

17 **(i) for purposes agreed upon between the data partners in the contract for data**
18 **pooling;**

19 **(ii) for purposes which the relevant data partner could reasonably expect to be**
20 **accepted by the other data partners, unless these purposes are inconsistent with**
21 **an agreement referred to in subparagraph (i); or**

22 **(iii) as necessary to comply with applicable law;**

23 **(b) A data partner may engage data processors, but may otherwise pass data from the**
24 **data pool, or data derived from such data, on to third parties only under the**
25 **conditions agreed upon between the data partners or required by applicable law;**

- 1 (c) As between the data partners, new intellectual property rights or similar rights
2 created with the use of data from the data pool belong to the partner or partners
3 who conducted the activity leading to the creation of the new right;
- 4 (d) If a data partner leaves the data pool, the data supplied by that data partner must
5 be returned to the relevant data partner, but data derived from the data, unless
6 essentially identical with the original data, remains in the pool. Upon leaving the
7 data pool, a data partner is entitled to a copy of any data in the pool that has been
8 derived, in whole or in substantial part, from data supplied by that data partner.
- 9 (4) In determining which rules and principles to apply by way of analogy, as provided in
10 Principle 5, to contracts for data pooling, consideration should be given to whether the
11 relationship between the data partners is one characterized by mutual trust and
12 confidence, such that the data partners owe each other fiduciary obligations, or, rather,
13 whether it is characterized by arm's length transactions with no fiduciary obligations.

Chapter C: Contracts for Services with regard to Data

Principle 12: Contracts for the processing of data

- 14 (1) A contract for the processing of data is one under which a processor undertakes to
15 process data on behalf of the controller. Such processing may include, inter alia:
- 16 (a) the collection and recording of data (e.g., data scraping);
17 (b) storage or retrieval of data (e.g., cloud space provision);
18 (c) analysis of data (e.g., data analytics services);
19 (d) organization, structuring, presentation, alteration or combination of data (e.g.,
20 data management services); or
21 (e) erasure of data.
- 22 (2) Subject to agreement of the parties and to rules that take priority under Principle 5, the
23 law should provide that the following terms are included in a contract for the processing
24 of data:

- 1 (a) The processor must follow the controller’s directions and act consistently with the
2 controller’s stated purposes for the processing;
- 3 (b) The processor must ensure at least the same level of data security and of
4 protection for the rights of third parties as the controller was under an obligation
5 to ensure, and must support the controller in complying with any legal obligations
6 for the protection of third parties that could reasonably be expected in a situation
7 of the relevant kind or of which the processor had notice when the contract was
8 made;
- 9 (c) The processor must not pass the data on to third parties;
- 10 (d) The processor may not process the data for the processor’s own purposes, except
11 to the extent reasonably necessary to improve the quality or efficiency of the
12 relevant service, so long as this does not harm the controller’s legitimate interests
13 and is not inconsistent with obligations for the protection of third parties within
14 the meaning of paragraph (2)(b); and
- 15 (e) Upon full performance or termination of the contract, the processor must transfer
16 to the controller any data resulting from the processing that has not already been
17 transferred. The processor must subsequently erase any data retained, except to
18 the extent reasonably necessary for existing or likely litigation or to the extent that
19 the processor has a legal right or obligation independent of these Principles to
20 keep the data beyond that time.
- 21 (3) In determining which rules and principles to apply directly or by way of analogy, as
22 provided in Principle 5, to contracts for processing of data, consideration should be
23 given to the nature of the service, such as to whether the focus is on changing the data
24 or on keeping it safe.

Principle 13: Data trust contracts

- 25 (1) A data trust contract is a contract among one or more controllers of data (the
26 ‘entrusters’) and a third party under which the entrusters empower the third party (the
27 ‘data trustee’) to make certain decisions about use or onward supply of data (the
28 ‘entrusted data’) on their behalf, in the furtherance of stated purposes that may benefit

1 the entrusters or a wider group of stakeholders (such entrusters or stakeholders being
2 referred to as the ‘beneficiaries’).

3 **(2) A data trust contract and the relationships it creates need not conform to any particular
4 organizational structure and need not include the characteristics and duties associated
5 with a common law trust. This Principle applies, with appropriate adjustments, to the
6 governing principles of any entity created pursuant to a data trust contract.**

7 **(3) Subject to agreement of the parties and to rules that take priority under Principle 5, the
8 law should provide that the following terms are included in a data trust contract or are
9 incorporated into the governing principles of any entity created pursuant to the data
10 trust contract:**

11 **(a) The data trustee is, subject to subparagraphs (b) and (c), empowered to make and
12 implement all decisions with regard to use or onward supply of the entrusted data,
13 including decisions concerning intellectual property rights and rights based on
14 data privacy/data protection law;**

15 **(b) The data trustee must act in furtherance of the stated purposes of the data trust
16 contract for the benefit of the beneficiaries and, even if the entrusters are not the
17 beneficiaries, in a manner that is not inconsistent with the legitimate interests of
18 the entrusters of which the data trustee has notice;**

19 **(c) The data trustee must follow any directions given by the entrusters, except to the
20 extent that the data trustee has notice that the directions are incompatible with the
21 stated or manifestly obvious purposes of the data trust;**

22 **(d) The data trustee must refrain from any use of the entrusted data for its own
23 purposes and must avoid any conflict-of-interest;**

24 **(e) The entrusters may terminate the data trustee’s power with regard to the data
25 entrusted by them at any time; however, this right may be limited to the extent
26 necessary to take into account reliance and similar legitimate interests of the
27 beneficiaries; and**

28 **(f) If the data trustee has retained any data entrusted, or any data derived from such
29 data, after the contract has come to an end (by termination or otherwise) the data**

1 trustee must return the data to the entrusters, and, when reasonable, take steps to
2 prevent further use of the data by onward recipients.

3 **(4) In determining which rules and principles to apply by way of analogy, as provided in**
4 **Principle 5, to data trust contracts, consideration should be given in particular to**

5 **(a) the stated purposes of the data trust contract and the nature of the data and of the**
6 **parties involved;**

7 **(b) whether the purposes of the data trust contract are primarily for the benefit of the**
8 **entrusters or broader constituencies; and**

9 **(c) the organizational structure of the relationships created by the data trust contract.**

Principle 14: Data escrow contracts

10 **(1) A data escrow contract is a contract among one or more parties planning to use data**
11 **(the ‘contracting parties’) and a third party (the ‘escrowee’) under which the escrowee**
12 **undertakes to make sure the powers and abilities of some or all of the contracting parties**
13 **with respect to the data are restricted (the ‘restricted parties’) so as to avoid conflict**
14 **with legal requirements, such as those imposed by antitrust law or data privacy/data**
15 **protection law.**

16 **(2) A data escrow contract and the relationships it creates need not conform to any**
17 **particular organizational structure. This Principle applies, with appropriate**
18 **adjustments, to the governing principles of any entity created pursuant to a data escrow**
19 **contract.**

20 **(3) Subject to agreement of the parties and to other principles that take priority under**
21 **Principle 5, the law should provide that the following terms are included in a data escrow**
22 **contract or are incorporated into the governing principles of any entity created pursuant**
23 **to the data escrow contract:**

24 **(a) The escrowee has such powers with regard to the data as are necessary for the**
25 **stated purpose of the data escrow contract;**

- 1 **(b) The escrowee must act in furtherance of the stated purposes of the data escrow**
2 **contract even if such action is inconsistent with interests of the contracting parties**
3 **that are distinct from the stated purpose of the data escrow contract;**
- 4 **(c) The escrowee must not follow any direction given by a contracting party that is**
5 **incompatible with the stated or manifestly obvious purpose of the data escrow**
6 **contract;**
- 7 **(d) The escrowee must refrain from any use or onward supply of the entrusted data**
8 **for its own purposes and must avoid any conflict of interest; and**
- 9 **(e) If the data escrow contract is terminated, each party has an obligation during the**
10 **winding-up of the relationship not to take actions that undermine the stated**
11 **purposes of the data escrow contract.**
- 12 **(4) In determining which rules and principles to apply by way of analogy, as provided in**
13 **Principle 5, to data escrow contracts, consideration should be given in particular to**
- 14 **(a) The stated purpose of the data escrow contract and the nature of the data and of**
15 **the parties involved; and**
- 16 **(b) The organizational structure of the relationships created by the data escrow**
17 **contract.**

Principle 15: Data marketplace contracts

- 18 **(1) A data marketplace contract is a contract between a party seeking to enter into a data**
19 **transaction (the ‘client’) and a data marketplace provider, under which the data**
20 **marketplace provider undertakes to enable or facilitate ‘matchmaking’ between the**
21 **client and other potential parties to data transactions and, in some cases, provide further**
22 **services facilitating the transaction.**
- 23 **(2) Subject to agreement of the parties and to other principles that take priority under**
24 **Principle 5, the law should provide that the following terms are included in a data**
25 **marketplace contract:**

- 1 **(a) Insofar as the data marketplace provider undertakes to facilitate or enable a**
2 **particular step with regard to a transaction, it must provide reasonable support to**
3 **the client in complying with any legal duties applicable to that step;**
- 4 **(b) The data marketplace provider must refrain from any use for its own purposes of**
5 **data, received from its client, that is the subject of the anticipated transaction; and**
- 6 **(c) Upon full performance or termination of the contract, the data marketplace**
7 **provider must erase any data in its control that is the subject of the anticipated**
8 **transaction and that it has received from its client, and any data derived from such**
9 **data.**
- 10 **(3) In determining which rules and principles to apply by way of analogy, as provided in**
11 **Principle 5, to data marketplace contracts, consideration should be given in particular**
12 **to:**
- 13 **(a) whether, and the degree to which, the data marketplace provider gains control of**
14 **the data concerned; and**
- 15 **(b) whether, and the extent to which, the payment or other performance owed to the**
16 **data marketplace provider depends on the whether the matchmaking results in a**
17 **data transaction.**

Part III: Data Rights

Chapter A: Rules and Principles Governing Data Rights

Principle 16: Data rights

- 18 **(1) Data rights may include the right to**
- 19 **(a) be provided access to data by means that may, in appropriate circumstances,**
20 **include porting the data;**
- 21 **(b) require the controller to desist from data activities;**
- 22 **(c) require the controller to correct data; or**

- 1 (d) receive an economic share in profits derived from the use of data.
- 2 (2) The data rights set out in Part III are not exhaustive; rather, a legal system may conclude
3 that parties should have additional rights of this sort. Accordingly, no negative inference
4 should be drawn from the absence of those rights in Part III.
- 5 (3) The rights set out in Part III are without prejudice to rights other than data rights that
6 a person may have against a controller of data with regard to that data, such as rights
7 arising from breach of contract, unjust enrichment, conversion of property rights, or
8 tort law.

Principle 17: Application of these Principles to data rights

- 9 Rights under Part III should be governed, in the following order of priority, by:
- 10 (a) rules of law that cannot be derogated from by agreement, including data
11 privacy/data protection law;
- 12 (b) agreement between the parties to the extent that the contract is consistent with
13 Principles 18 to 27 or there is freedom of the parties to derogate from Principles 18
14 to 27 under the applicable law;
- 15 (c) any applicable rules of the law other than those referred to in clause (a) that have
16 been developed for application to data rights; and
- 17 (d) Principles 18 to 27.

Chapter B: Data Rights with Regard to Co-Generated Data

Principle 18: Co-generated data

- 18 (1) Factors to be taken into account in determining whether, and to what extent, data is to
19 be treated as co-generated by a party within the meaning of Principles 19 to 23 are, in
20 the following order of priority:
- 21 (a) the extent to which that party is the subject of the information coded in the data,
22 or is the owner or operator of an asset that is the subject of that information;

- 1 (b) the extent to which the data was produced by an activity of that party, or by use of
2 a product or service owned or operated by that party;
- 3 (c) the extent to which the data was collected or assembled by that party in a way that
4 creates something of a new quality; and
- 5 (d) the extent to which the data was generated by use of a computer program or other
6 relevant element of a product or service, which that party has produced or
7 developed.
- 8 (2) Factors to be considered when assessing the extent of a contribution include the type of
9 the contribution, the magnitude of the contribution (including by way of investment),
10 the proximity or remoteness of the contribution, the degree of specificity of the
11 contribution, and the contributions of other parties.
- 12 (3) Contributions of a party that are insignificant in the circumstances do not lead to data
13 being considered as co-generated by that party.

Principle 19: General factors determining rights in co-generated data

- 14 (1) Data rights in co-generated data arise from considerations of fairness; accordingly, the
15 way they are incorporated in existing legal frameworks under applicable law and the
16 extent to which they may be waived or varied by agreement should be determined by
17 the role such considerations of fairness play in the relevant legal system.
- 18 (2) In the case of co-generated data, a party who had a role in the generation of the data has
19 a data right when it is appropriate under the facts and circumstances, which is
20 determined by consideration of the following factors:
- 21 (a) the share which that party had in the generation of the relevant data, considering
22 the factors listed in Principle 18;
- 23 (b) the weight of grounds such as those listed in Principles 20 to 23 which that party
24 can put forward for being afforded the data right;
- 25 (c) the weight of any legitimate interests the controller or a third party may have in
26 denying the data right;

1 (d) imbalance of bargaining power between the parties; and

2 (e) any public interest, including the interest to ensure fair and effective competition.

3 (3) The factors listed in paragraph (2) should also be taken into account for determining
4 the specifications or restrictions of data rights, such as concerning data formats, timing,
5 data security, further support required for exercise of the right to be fully effective, and
6 remuneration to be paid.

Principle 20: Access or porting with regard to co-generated data

7 (1) Grounds that, subject to Principle 19, may give rise to a right to access or to port co-
8 generated data include circumstances in which the access or porting is

9 (a) necessary for normal use, maintenance or re-sale by the user of a product or
10 service consistent with its purpose and the controller is part of the supply network
11 and can reasonably be expected to have foreseen this necessity;

12 (b) necessary for quality monitoring or improvement by the supplier of a product or
13 service consistent with duties of that supplier and the controller is part of the
14 supply network and can reasonably be expected to have foreseen this necessity;

15 (c) necessary for establishing facts, such as for better understanding by a party of that
16 party's own operations, including any proof of such operations that party needs to
17 give vis-à-vis a third party, where this is urgently needed by that party and the
18 access to or porting of the co-generated data cannot reasonably be expected to
19 harm the controller's interests;

20 (d) necessary for the development of a new product or service by a party where such
21 development was, in the light of that party's and the controller's previous business
22 operations, the type of their respective contributions to the generation of the data,
23 and the nature of their relationship, to be seen primarily as a business opportunity
24 of that first party; or

25 (e) necessary for the avoidance of anti-competitive lock-in effects to the detriment of a
26 party, such as by preventing that party from rightfully switching suppliers of
27 products or services or attracting further customers.

1 (2) Consistent with Principle 19(3), a right under paragraph (1) should be afforded only
2 with appropriate restrictions such as disclosure to a trusted third party, disaggregation,
3 anonymisation or blurring of data, to the extent that affording the right without such
4 restrictions would be incompatible with the rights of others, or with public interests.

5 (3) The controller must comply with the duties under Principles 32 for the protection of
6 third parties, and restrictions under paragraph (2) must in any case enable the
7 controller to do so.

Principle 21: Desistance from data activities with regard to co-generated data

8 Grounds that, subject to Principle 19, may give rise to a party's right to require that the
9 controller desist from data activities with regard to co-generated data, up to a right to
10 require erasure of data, should include situations in which

11 (a) the data activities cause, or can reasonably be expected to cause, significant harm,
12 including non-economic harm, to that party; and

13 (b) the purpose of the data activities is inconsistent with the way that party
14 contributed to the generation of the data, in particular because

15 (i) that party was induced to contribute to the generation of the data for an entirely
16 different purpose and could not reasonably have been expected to contribute to
17 the generation of the data if it had known or foreseen the purpose of the data
18 activities engaged in by the controller; or

19 (ii) that party's assent to its contribution to the generation of the data for that
20 purpose was obtained in a manner that is incompatible with doctrines that
21 vindicate important public policies including those that protect parties from
22 overreaching conduct or agreements.

Principle 22: Correction of co-generated data

23 Grounds that, subject to Principle 19, may give rise to a party's right to require that the
24 controller correct errors in co-generated data, including incompleteness of the data,
25 should include situations in which control or processing of the incorrect data may cause

1 more than insignificant harm, including non-economic harm, to that party's or another
2 party's legitimate interests, and the costs of correction are not disproportionate to the
3 harm that might otherwise result.

Principle 23: Economic share in profits derived from co-generated data

4 (1) A party is normally not entitled to an economic share in profits derived by another party
5 from the use of co-generated data unless there is a contractual or statutory basis for such
6 a claim or it is part of an individual arrangement under Principle 19(3).

7 (2) Notwithstanding paragraph (1), in exceptional cases a party may be entitled to an
8 economic share in profits derived by a controller of co-generated data from use of the
9 data when

10 (a) that party's contribution to the generation of the data

11 (i) was sufficiently unique that it cannot, from an economic point of view, be
12 substituted by contributions of other parties; or

13 (ii) caused that party significant effort or expense; and

14 (b) profits derived by the controller are exceptionally high; and

15 (c) the party seeking an economic share was, when its contribution to the generation
16 of the data was made, not in a position to bargain effectively for remuneration.

Chapter C: Data Rights for the Public Interest

Principle 24: Justification for data rights and obligations

17 (1) The law should afford data rights for the public interest, and for similar reasons
18 independent of the share that the party to whom the rights are afforded had in the
19 generation of the data, only if the encroachment on the controller's or any third party's
20 legitimate interests is necessary, suitable and proportionate to the public interest
21 pursued.

22 (2) Paragraph (1) is not intended to address intergovernmental relations.

- 1 **(3) The proportionality test referred to in paragraph (1) should apply also for determining**
2 **the specifications or restrictions of data rights, such as concerning data formats, timing,**
3 **data security, further support required for exercise of the right to be fully effective, and**
4 **remuneration to be paid.**
- 5 **(4) If the law does not afford a data right but imposes a functionally equivalent data sharing**
6 **obligation, the Principles under this Chapter apply with appropriate adjustments.**

Principle 25: Granting of data access by the controller

- 7 **(1) If the law affords a data access right within the meaning of Principle 24, the law should**
8 **provide that the controller must provide access under conditions that are fair,**
9 **reasonable and non-discriminatory within the class of parties that have been afforded**
10 **the right.**
- 11 **(2) Consistent with Principle 24(3), a data access right should be afforded only with**
12 **appropriate restrictions such as disclosure to a trusted third party, disaggregation,**
13 **anonymization or blurring of data, to the extent that affording the right without such**
14 **restrictions would be incompatible with the rights of others, or with public interests.**
- 15 **(3) The controller must comply with the duties under Principles 32 for the protection of**
16 **third parties, and restrictions under paragraph (2) must in any case enable the**
17 **controller to do so.**

Principle 26: Data activities by recipient

- 18 **(1) If the law affords a data access right within the meaning of Principle 24 to a party, the**
19 **law should provide that, subject to paragraph (2), the party may utilize the data it**
20 **receives in any lawful way and for any lawful purpose that is not inconsistent with**
- 21 **(a) the public interest for which the right was afforded, provided the recipient had**
22 **notice of that interest;**
- 23 **(b) restrictions for the protection of others imposed under Principle 25(2); or**

1 (c) any agreement between the parties, including an agreement concerning duties and
2 restrictions imposed by the controller on the recipient under Principle 32.

3 (2) A party to whom a data access right is afforded under Principle 24 may not utilize that
4 data in a way that harms the legitimate interests of the original controller more than is
5 inherent in the purpose for which the right was afforded.

Principle 27: Reciprocity

6 If the law affords a data access right within the meaning of Principle 24 to a party against
7 a controller, this is a strong argument for affording a similar data access right to the
8 original controller against the first party under comparable circumstances. Whether
9 this argument should prevail depends, inter alia, on whether affording such a reciprocal
10 right would be inconsistent with the purpose of provision of access to the first party.

Part IV: Third Party Aspects of Data Activities

Chapter A: Protection of Others against Data Activities

Principle 28: Wrongfulness of data activities vis-à-vis another party

11 (1) Data activities are wrongful vis-à-vis another party (a ‘protected party’) if:

12 (a) they interfere with any right of the protected party that has third-party effect per
13 se within the meaning of Principle 29;

14 (b) they do not comply with contractual limitations on data activities, enforceable by
15 the protected party, of the sort described in Principle 30; or

16 (c) access to the data has been obtained from the protected party by unauthorized
17 means within the meaning of Principle 31.

18 (2) In assessing whether data activities are wrongful, the conditions under which these
19 activities are pursued, such as provision of an adequate level of data security or
20 compliance with any duty under Principle 32, should be taken into account.

1 (3) Implementation of this rule should take into account applicable doctrines of
2 justification, such as freedom of information and expression.

Principle 29: Rights that have third-party effect per se

3 (1) For the purpose of Principle 28(1)(a), rights that have third-party effect per se include
4 the following:

5 (a) intellectual property rights and similar rights;

6 (b) data privacy/data protection rights and similar rights; and

7 (c) any other rights that, under the applicable law, have similar third-party effects.

8 (2) The extent to which rights within the meaning of paragraph (1) limit data activities, as
9 well as the effect of such limitations, is determined by the applicable law.

Principle 30: Contractual limitations

10 (1) For the purpose of Principle 28(1)(b), a contractual limitation on data activities is a
11 contractual term that limits data activities of any party to the contract, including by
12 limiting the use or onward transfer of data.

13 (2) In determining whether a contractual limitation on data activities is in conflict with
14 mandatory rules of law that vindicate important public policies and those that protect
15 parties from overreaching conduct or agreements, factors to be taken into account
16 include whether the agreement

17 (a) unduly limits the freedoms of a contracting party, taking into account, inter alia,
18 comparable limits of intellectual property protection;

19 (b) unduly limits activities in the public interest; or

20 (c) has unjustified discriminatory or anti-competitive effects.

Principle 31: Unauthorized access

1 (1) For the purpose of Principle 28(1)(c), access to data has been obtained by unauthorized
2 means if it has been obtained by:

- 3 (a) circumvention of security measures;
- 4 (b) taking advantage of an obvious mistake, such as security gaps that the person
5 accessing the data could not reasonably believe the controller had intended; or
- 6 (c) interception by technical means of non-public transmissions of data, including
7 electromagnetic emissions from a medium carrying data.

8 (2) Access to data has not been obtained by unauthorized means if

- 9 (a) access to the data is allowed under an agreement between the person accessing the
10 data and the controller; or
- 11 (b) the person accessing the data had a right that, under other law (such as law
12 relating to freedom of information and expression), prevails over the controller's
13 right under this Principle.

Chapter B: Effects of Onward Supply on the Protection of Others

Principle 32: Duties of a supplier in the context of onward supply

14 (1) Where a party supplying data to a recipient may pass the data on but is obligated to
15 comply with duties and restrictions within the meaning of Chapter A, the law should
16 require the supplier to

- 17 (a) impose the same duties and restrictions on the recipient (unless the recipient is
18 already bound by them), including the duty to do the same if the recipient supplies
19 the data to other parties; and
- 20 (b) take reasonable and appropriate steps (including technical safeguards) to assure
21 that the recipient, and any parties to whom the recipient may supply the data, will
22 comply with those restrictions.

- 1 (2) Where the supplier later obtains knowledge of facts that indicate wrongful data
2 activities within the meaning of Principle 28 on the part of a recipient, or that render
3 data activities by the recipient wrongful or would otherwise require steps to be taken
4 for the benefit of a protected party, the supplier must take reasonable and appropriate
5 measures to stop wrongful activities or to take such other steps as are appropriate for
6 the benefit of a protected party.
- 7 (3) Nothing in this Principle precludes strict vicarious liability of a controller for data
8 activities by a processor under the applicable law.
- 9 (4) Whether the supplier's duties under this Principle may be waived by the protected party
10 or varied by agreement to the detriment of that party is determined by the nature of the
11 relevant duties and restrictions under Chapter A and any applicable rules of law that
12 make those duties non-waivable by the protected party.

Principle 33: Direct action against downstream recipient

13 Where an immediate recipient of data had a duty under Principle 32 vis-à-vis its supplier
14 to impose particular terms on a downstream recipient to whom the immediate recipient
15 will supply the data, and where the immediate recipient has complied with that duty but
16 the downstream recipient breaches the terms imposed on it, the initial supplier may
17 proceed directly against the downstream recipient after giving notice to the immediate
18 recipient.

Principle 34: Wrongfulness taking effect vis-à-vis downstream recipient

- 19 (1) In addition to wrongfulness following directly from Chapter A, a data activity by a
20 downstream recipient that has received the data from a supplier is wrongful where (i)
21 control by that supplier was wrongful, (ii) that supplier acted wrongfully in passing the
22 data on, or (iii) that supplier acted wrongfully in failing to impose a duty or restriction
23 on the downstream recipient under Principle 32 that would have excluded the data
24 activity, and the downstream recipient either

- 1 **(a) has notice of the wrongfulness on the part of the supplier at the time when the data**
2 **activity is conducted; or**
- 3 **(b) failed to make such investigation when the data was received as could reasonably**
4 **be expected under the circumstances.**
- 5 **(2) Paragraph (1) does not apply where**
- 6 **(a) wrongfulness on the part of the supplier was not material in the circumstances and**
7 **could not reasonably be expected to cause material harm to a party protected**
8 **under Chapter A;**
- 9 **(b) the downstream recipient obtained notice only at a time after the data was**
10 **supplied, and the downstream recipient’s reliance interests clearly outweigh, in the**
11 **circumstances, the legitimate interests of a party protected under Chapter A; or**
- 12 **(c) the data was generally accessible to persons that normally deal with the kind of**
13 **information in question.**
- 14 **(3) Paragraphs (1) and (2) apply, with appropriate adjustments, to data activities by a party**
15 **that has not received the data from a supplier but that has otherwise obtained access to**
16 **the data through another party.**

Chapter C: Effects of Other Data Activities on the Protection of Third Parties

Principle 35: Duties of a controller with regard to data processing and derived data

- 17 **(1) If a controller may process data but is obligated to comply with duties and restrictions**
18 **within the meaning of Chapter A, the controller must, when processing that data,**
19 **exercise such care that is reasonable under the circumstances in**
- 20 **(a) determining means and purposes of processing that are compatible with the duties**
21 **and restrictions; and**
- 22 **(b) ascertaining which duties and restrictions apply with regard to the derived data**
23 **and taking reasonable and appropriate steps to make sure the duties and**
24 **restrictions are complied with.**

- 1 **(2) Whether duties and restrictions with regard to the original data also apply with regard**
2 **to derived data, or whether lesser or additional duties and restrictions apply, is to be**
3 **determined by the rules and principles governing the relevant source of protection**
4 **under Chapter A. In a case of doubt, considerations to be taken into account include:**
- 5 **(a) the degree to which the derived data is different from the original data, such as**
6 **whether the original data can be reconstructed from the derived data by way of**
7 **reasonable steps of disaggregation or reverse engineering; and**
- 8 **(b) the degree to which the derived data poses a risk for a protected party as**
9 **compared with the risk posed by the original data.**
- 10 **(3) If processing the original data was not wrongful, but subsequent events occur that would**
11 **make the same type of processing wrongful, this does not retroactively make the prior**
12 **processing wrongful.**

Principle 36: Wrongful processing

- 13 **(1) Where processing data was wrongful, the controller must take all reasonable and**
14 **appropriate steps to undo the processing, such as by disaggregating data or deleting**
15 **derived data, even where duties and restrictions under Chapters A and B do not apply,**
16 **in accordance with Principle 35, with regard to derived data.**
- 17 **(2) To the extent that undoing the processing in cases covered by paragraph (1) is not**
18 **possible or would mean a destruction of values that is unreasonable in light of the**
19 **circumstances giving rise to wrongfulness on the part of the controller and the legitimate**
20 **interests of any party protected under Chapter A, an allowance may be made in money**
21 **whenever and to the extent this is reasonable in the circumstances and may be combined**
22 **with restrictions on further use of the derived data. Factors to be taken into account**
23 **include**
- 24 **(a) whether the controller had notice of the wrongfulness at the time of processing;**
25 **(b) the purposes of the processing;**
- 26 **(c) whether wrongfulness was material in the circumstances or could be expected to**
27 **cause relevant material harm to a party protected under Chapter A; and**

1 (d) the amount of investment made in processing, and the relative contribution of the
2 original data to the derived data.

3 (3) Paragraphs (1) and (2) apply with appropriate adjustments to products or services
4 developed with the help of the original data.

Principle 37: Effect of non-material non-compliance

5 (1) If a controller engages in data activities with respect to a large data set, and the data
6 activities do not comply with duties and restrictions under Chapter A with regard to
7 some of the data, the law should provide that such activities are not wrongful with
8 regard to the whole data set if

9 (a) the non-compliance is not material in the circumstances, such as when the affected
10 data is only an insignificant portion of the data set with regard to which data
11 activities take place;

12 (b) the controller has made the efforts that could reasonably be expected in the
13 circumstances to comply with the duties and restrictions; and

14 (c) the data activities are not related to the purpose for which duties or restrictions
15 under Chapter A are imposed and could not reasonably be expected to cause
16 material harm to a protected party.

17 (2) When paragraph (1) applies, the controller must, upon obtaining notice, remove the
18 affected data from the data set for the purpose of future data activities unless this is
19 unreasonable in the circumstances.

Part V: Multi-State Issues

Principle 38: Application of established choice-of-law rules of the forum

20 (1) When an issue is within the territorial scope of the law of more than one State, the law
21 applicable to that issue is determined by the forum's choice of law rules. These Principles
22 do not determine the territorial scope of a State's law.

1 (2) The law applicable to data contracts under Part II should be the law of the State that
2 would be selected under the forum’s choice of law rules for contracts.

3 (3) For any other issue arising under these Principles, the law applicable to that issue should
4 be

5 (a) the law of the State that would be selected under the forum’s choice of law rules if
6 those rules provide a clear rule for determining the law applicable to that issue; or

7 (b) if the forum’s choice of law rules do not provide a clear rule for determining the
8 law applicable to that issue, the law determined by application of Principle 39.

Principle 39: Issues not covered by established choice of law rules of the forum

9 (1) The law applicable to issues not already covered by Principle 38 should be the law of the
10 State that has the most significant relationship to the legal issue in question. Contacts to
11 be taken into account in determining which State has the most significant relationship
12 include:

13 (a) the place where data activities (i) are designed to produce effects on relevant
14 interests or (ii) actually produce effects;

15 (b) the domicile, residence, nationality, place of incorporation and place of business of
16 the party asserting a right and the party against whom it is asserted; and

17 (c) the law of the State that governs a pre-existing legal relationship, if any, between
18 the party asserting a right and the party against whom it is asserted; and

19 (d) the place where the data is generated.

20 (2) Parties may, by mutual agreement made after a dispute has arisen, choose the State
21 whose law will govern their legal relationship with regard to a legal issue addressed by
22 these Principles, unless this is incompatible with the nature of the legal issue or
23 considerations of public policy.

Principle 40: Relevance of storage location

- 1 **(1) Except as provided in paragraph (2), for choice-of-law purposes the location of the**
2 **storage of data is relevant as a connecting factor only when the issue in question relates**
3 **to storage or to rights in the medium.**
- 4 **(2) The location of storage of data may be relevant for choice-of-law purposes as a**
5 **connecting factor of a residual nature, such as in the absence of other connecting factors**
6 **or when consideration of other connecting factors is indeterminate.**
- 7 **(3) The fact that data is stored outside a State does not of itself ordinarily raise issues of**
8 **extraterritorial exercise of jurisdiction or application of law as long as there are**
9 **sufficient links between the State and the activities with respect to the data it seeks to**
10 **regulate or the entitlements with respect to the data it seeks to enforce.**
- 11