



General Assembly

Distr.: Limited
4 February 2026

Original: English

**United Nations Commission on
International Trade Law**
Working Group IV (Electronic Commerce)
Seventieth session
New York, 23–27 March 2026

Draft model legislative provisions on contracts for the provision of data: Explanatory note

Note by the Secretariat

Contents

	<i>Page</i>
I. Introduction	2
II. Article-by-article remarks	2
A. Article 1. Definitions	2
B. Article 2. Scope of application	3
C. Article 3. Party autonomy	6
D. Article 4. Interpretation	6
E. Article 5. Obligation to provide the data	7
F. Article 6. Mode of provision of the data	7
G. Article 7. Timing of provision of the data	9
H. Article 8. Conformity of the data	9
I. Article 9. Use of the data	11
J. Article 10. Derived data	14
K. Article 11. Common obligations of the data provider and data recipient	14
L. Article 12. Non-performance	14
M. Article 13. Passive provision of data	15



I. Introduction

1. This note contains article-by-article remarks on the draft model legislative provisions contained in [A/CN.9/WG.IV/WP.192](#) (hereafter referred to collectively as “the text”). In line with explanatory notes on other UNCITRAL texts prepared by the Working Group, these remarks will constitute the main part of an eventual explanatory note on the text.

2. It is anticipated that an introductory section will be inserted once the form of the text is decided. That section will outline the objectives of the text, its background and drafting history, and the key concepts and principles on which it is based. It will draw on existing material in notes prepared by the UNCITRAL secretariat for the Working Group and Commission, including on matters such as: (i) data as an item of trade, (ii) the significance of the intangibility and non-rivalrousness of data, (iii) the concepts of “data transactions” and “data rights” and the different roles played by data providers and data recipients in the “data ecosystem”, (iv) the interaction of the provisions with the United Nations Convention on Contracts for the International Sale of Goods (CISG) and other international data initiatives, and (v) the approach taken by the Working Group with regard to the concepts from other legal regimes, such as “sales”, “ownership” and the “control” of data.¹

II. Article-by-article remarks

A. Article 1. Definitions

3. The definition of “data” in article 1 is broad and inclusive. It is complemented by article 2, which delimits the scope of the text by reference to particular transactions in data and particular types of data.

4. The concept of data as a “representation of information” is based on the widely-used definition of “data”, formulated by the International Organization for Standardization (ISO), as “a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing”.² A similar understanding of data underlies the concept of “data message” in UNCITRAL texts on electronic commerce.

5. Unlike the ISO definition, which acknowledges that data need not be in electronic form and can be processed both by humans and by automated means, the definition in article 1 requires data to be in “electronic form or other form suitable for processing in an information system”. This requirement encompasses data in digital form (i.e. information represented by a string of “zeros” and “ones”). However, consistent with the principle of technology neutrality, the definition encompasses data suitable for processing using other information technologies (e.g. high-speed analogue computing and quantum computing).

6. The requirement for data to be in electronic form (or other form suitable for processing in an information system) underscores the importance of automated processing (i.e. processing by an automated system or machine) to the value of data in the digital economy. The definition does not expressly require data to be in a machine-readable form, as such a requirement could be understood in some legal systems to be a matter of data conformity (e.g. that the data be in a particular format, such as to allow the information to be extracted using commonly available software applications).

7. The definition refers to the processing of data in an “information system”. This term is borrowed from the Model Law on Electronic Commerce (MLEC), where it is

¹ See, e.g. [A/CN.9/1117](#), paras. 3–6, 10, 15–21, 26–31 and 46–54, [A/CN.9/WG.IV/WP.180](#), paras. 21, 22–24, 42 and 47–51, and [A/CN.9/WG.IV/WP.188](#), paras. 3–10.

² ISO, *Information Technology – Vocabulary*, ISO/IEC Standard No. 2382, 2015.

defined to mean “a system for generating, sending, receiving, storing or otherwise processing data messages” and covers the entire range of technical means used for transmitting, receiving and storing information. The term comprises hardware and software components, including data-generating devices connected to the system (i.e. “connected devices”), Internet connection and software for data analytics.

References

[A/CN.9/1093](#), para. 85; [A/CN.9/1132](#), paras. 18–23; [A/CN.9/1162](#), para. 88; [A/CN.9/1197](#), paras. 31–32, 67; [A/CN.9/1241](#), para. 22.

B. Article 2. Scope of application

1. “Contracts for the provision of data” (paragraph 1)

8. Paragraph 1 states that the rules apply to “contracts”. By implication, the rules apply to the voluntary provision of data, and do not apply to the provision of data that is mandated by law outside a contractual setting. The text does not address matters relating to contract formation or validity [as confirmed in paragraph 4].

9. Paragraph 1 refers to contracts “for the provision of data”, which is intended to cover a broad range of transactions in data. It includes transactions that may be described as data “supply” or data-“sharing” arrangements. As the terms “supply” and “sharing” can imply a particular regime for the use of the data by the parties, the text uses “provision” as a more neutral term. Contracts for the provision of data may not belong to any recognized type of contract under national law or may exhibit characteristics of different types. The text does not characterize the provision of data as either “sales” or “licences” and avoids terminology associated with such transactions. Nor does it attempt to prescribe transactions that are deemed to be contracts for the provision of data. The drafters intended the text to accommodate a variety of business practices and recognized that those practices were evolving.

10. While the concept of the provision of data is not defined, paragraph 1 expressly acknowledges that it may involve a third party, such as the operator of a data exchange. Other provisions also give meaning to the term. For instance, article 5 equates the provision of data with the data provider “making the data available”, which presupposes that the data provider has some control over how the data is processed, although it does not require the data provider to “hold” the data. Article 6(2)(a) contemplates that the data may be made available without being transmitted between different information systems, and article 7 contemplates the provision of data as a one-off delivery, at regular intervals (e.g. whenever updates are available) or continuously (e.g. data generated by a connected device).

11. The text was developed with reference to the Principles for a Data Economy, jointly developed by the American Law Institute and European Law Institute (hereafter the “ALI/ELI Principles”),³ which identify five types of “contracts for the supply or sharing of data”, namely:

(a) “Contracts for the transfer of data”, under which the supplier puts the data recipient in control of data by transferring the data to a medium within the data recipient’s control, or by delivering to the recipient a medium on which the data is stored;

(b) “Contracts for simple access to data”, under which the recipient is given access to the data on a medium within the supplier’s control;

³ The ALI/ELI Principles were presented to the Working Group at its sixty-third session: see [A/CN.9/1093](#), paras. 82–85.

(c) “Contracts for exploitation of a data source”, under which the data recipient is given access to a device or facility by which data is collected or otherwise generated;

(d) “Contracts for authorization to access”, under which the data recipient is authorized to access data; and

(e) “Contracts for data pooling”, under which two or more parties share data in a “data pool” (with or without the involvement of a third-party intermediary).

12. The text is intended to accommodate each of these types of contracts. Thus, a contract under which data is provided in exchange for data, as in the case of a decentralized data pool, would be captured by paragraph 1, as would a contract under which data is provided through a third-party intermediary, as in the case of a centralized data pool or data exchange.

13. It is important to stress that paragraph 1 does not cover every contract under which data is provided. It is only concerned with contracts where the provision of data forms the object of the contract. Thus, a contract under which a party provides data processing services (e.g. data scraping, cloud-based services, data analytics and electronic transmission services) would not ordinarily be captured by paragraph 1, nor would a contract for the supply of goods or services merely because of incidental information-sharing obligations that are capable of being performed by electronic means, or because data is provided as counter-performance. In that regard, paragraph 1 is complemented by paragraph 2, which expressly excludes contracts that might otherwise be considered contracts for the provision of data.

14. The line between contracts for data processing services and contracts for the provision of data is not always clear-cut. For instance, data may be provided together with the means for using the data, including under a “data-as-a-service” model (e.g. via an online platform for processing the data). Moreover, the data provider may undertake to produce the data that is provided (e.g. by generating the data or by collecting and combining other data). However, the drafters purposefully did not include a provision inspired by article 3(2) of the CISG, whereby contracts in which the “preponderant part” of the obligations of the data provider consisted in the supply of services would be excluded from scope. In practice, the provision of data is sometimes regarded in itself as a “service”, particularly where it is provided in real-time. The text does not take a position on whether contracts for the provision of data should be characterized as the supply of services.

2. Functional and representative data (paragraph 2)

15. Paragraph 2 is designed to exclude from scope transactions in “functional data” (e.g. software) and “representative data” (e.g. digital assets). These terms are not used in the text as it was felt that they had not become universally established legal concepts at the time of drafting, despite featuring in the ALI/ELI Principles. Subparagraphs (a) and (b) are based on the definitions of those terms set out in Principle 2 of the ALI/ELI Principles, respectively. Subparagraph (b) refers not only to data representing “value” but also “rights” that are acquired by a person by virtue of their association with the data, such as by holding or controlling the data. The existence of such rights and their acquisition, as well as the nature of the association between the rightsholder and the data, are left to applicable law outside the text.

16. The exclusion in paragraph 2 is justified on several grounds. First, transactions in functional and representative data are not concerned with data itself (i.e. the information that the data represents), but with the functions that it delivers (e.g. a computer program) or the rights or value that holding or controlling the data represents (e.g. data comprising a unit of cryptocurrency, an electronic transferable record, an electronic warehouse receipt, or an electronic negotiable cargo document). The same may be said for transactions in digital content (e.g. consumable content delivered by integrating data into the user’s digital environment), as well as the exchange of data in the delivery of “trust services” within the meaning of the Model

Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT). The provisions, particularly those on data conformity (article 8) and data use (article 9) are not adapted to such transactions. For instance, the list of relevant characteristics of data quality in article 8(4) does not include functionality, compatibility or interoperability, which are more appropriate for software and digital content, while the use rights regime in article 9 does not sit comfortably with holding a digital asset in a system that assures the singularity and control of the data comprising that asset.

17. Second, transactions in functional data such as software belong to a well-established type of contract in various legal systems with which the text need not interfere. Similarly, transactions in certain types of functional and representative data may be the subject of specific regulation in several jurisdictions, thus engaging the “give way” rule in article 2(4) and effectively making the text redundant for those transactions.

18. Paragraph 2 is stated to be “without prejudice to paragraph 1”, which acknowledges that some transactions in functional and representative data may already be excluded by paragraph 1 (see para. 13 above). It also acknowledges that some data transactions that are not concerned with the data itself might not fall within either subparagraph (a) and (b), particularly in view of evolving business practices and advances in digital technologies.

3. Contracts with consumers (paragraph 3)

19. *[To be inserted if article 2(3) is retained, drawing on A/CN.9/WG.IV/WP.186, para. 22, and the deliberations of the Working Group (e.g. A/CN.9/1197, paras. 37–40 and A/CN.9/1241, paras. 33–36)].*

4. Preserving other laws (paragraph 4)

20. Paragraph 4 operates as a “give way” clause in the event of conflict between the text, as enacted, and other laws. Unlike paragraphs 2 and 3, it is not intended to exclude matters from scope; to the extent that other laws do not conflict with the text, its provisions apply on their terms. Accordingly, for instance, the mere fact that the provision of the data infringes laws on data privacy and protection does not mean that the data recipient has no recourse to article 8(3)(a). At the same time, the text only applies to the rights and obligations of the parties and not to other matters relating to the validity of the contract and on the effect of its provisions on rights or obligations under other laws, including rights of a proprietary nature.

21. Paragraph 4 is modelled on article 2(4) of the MLIT. It is intended primarily to clarify that the draft rules do not affect the application of rules of mandatory law from which the parties cannot derogate under article 3. It contains an illustrative, non-exhaustive list of laws that may apply to prohibit or limit the provision or use of data. The reference to intellectual property encompasses copyright and database rights. Other laws that may be captured by paragraph 4 include national security laws. Paragraph 4 applies not only to laws specifically governing data transactions or information handling, but also to other laws of general application that may apply in the context of data transactions, such as constitutional safeguards or laws on matters of public policy.

22. The term “rule of law” carries the same meaning as in other UNCITRAL texts on electronic commerce, and is therefore intended to encompass statutory, regulatory and judicially created laws as well as procedural laws.

23. By virtue of paragraph 4, the text avoids the impracticality – if not impossibility – of limiting the application of its provisions to data other than personal data, while ensuring that protective and regulatory measures regarding personal data continue to apply with full force. It also avoids excluding from scope the variety of data that might be subject to intellectual property rights. The text does not address measures to be taken by the parties to comply with the particular requirements of personal data

and intellectual property law. If any of the provisions need to be varied to accommodate the particular arrangement between the parties as to the exploitation of intellectual property rights or the processing of personal data, this can be done under article 3.

24. Paragraph 4 does not define “data privacy and protection” or “consumer protection”, which are left to applicable law outside the text. [The concept of “consumer protection” might not be coextensive with persons referred to in paragraph 3.]

References

[A/77/17](#), paras. 161–162; [A/78/17](#), para. 159.

[A/CN.9/1093](#), paras. 78, 87–89, 92; [A/CN.9/1132](#), paras. 9, 18–19, 24; [A/CN.9/1162](#), paras. 61, 63–70; [A/CN.9/1197](#), paras. 33–41, 67; [A/CN.9/1202](#), para. 76; [A/CN.9/1241](#), paras. 26–38.

C. Article 3. Party autonomy

25. Party autonomy is a fundamental principle underpinning commercial law and UNCITRAL texts. It aims to promote international trade, as well as technological innovation and the development of new business practices. Article 3 draws on article 6 of the CISG and article 4 of the Model Law on Electronic Transferable Records (MLETR). Like in those texts, party autonomy operates within the limits of mandatory law. In the context of data transactions, the drafters were conscious that rules of mandatory law, such as laws on data privacy and protection, can engage matters of public policy. For that reason, paragraph 1 is stated to apply “subject to article 2, paragraph 4”.

26. Paragraph 2 clarifies that party autonomy operates only as between the parties. At the same time, consistent with the approach taken in other UNCITRAL texts on electronic commerce, the agreement need not be manifested in a contract between the parties but may, for instance, be manifested in their mutual assent to the rules of a data exchange operated by a third party that sets the conditions for the provision of data via the platform.

27. Several provisions apply subject to the agreement of the parties (“unless otherwise agreed”) or anticipate such agreement (“as agreed”). While such statements might be seen as redundant in view of article 3, it was felt that such prescriptions serve a useful purpose in clarifying the application of the text.

References

[A/CN.9/1093](#), para. 95; [A/CN.9/1132](#), para. 14; [A/CN.9/1162](#), para. 84; [A/CN.9/1197](#), para. 42; [A/CN.9/1202](#), para. 57; [A/CN.9/1241](#), para. 39.

D. Article 4. Interpretation

28. Article 4 is based on article 3 of the MLEC, which in turn reflects a provision that is commonly found in other UNCITRAL texts on electronic commerce and beyond (see, for example, article 7 of the CISG). It aims to promote uniform interpretation of the text across enacting jurisdictions and to limit the extent to which those rules, once enacted, are interpreted solely by reference to domestic law concepts.

29. Paragraph 1 draws the attention of judges and other adjudicators to the international origin of the text as enacted. Decisions originating from other enacting jurisdictions may therefore be particularly relevant.

30. Paragraph 2 requires any gaps in the text as enacted to be filled by reference to the “general principles” on which it is based. Several principles were cited during the development of the rules, including party autonomy, good faith, equity and technology neutrality. In addition, certain assumptions about data and data transactions that were identified during the development of the text (see [[A/CN.9/WG.IV/WP.183](#), para. 30]) may provide guidance in filling gaps.

References

[A/CN.9/1093](#), para. 95; [A/CN.9/1132](#), para. 14; [A/CN.9/1197](#), para. 43; [A/CN.9/1202](#), paras. 15 and 73; [A/CN.9/1241](#), para. 40.

E. Article 5. Obligation to provide the data

31. Inspired by the structure of the CISG, the text contains separate provisions on the general obligation to provide the data (article 5), the mode of provision (article 6), and the conformity of the data (article 8).

32. Paragraph 1 of article 5 establishes a general obligation on the data provider to provide the data. Paragraph 2 states that the essential component of that obligation is to make the data available to the data recipient.

33. Whether data is “available” is a factual matter that is concerned with whether the data recipient is in a position to use the data. However, consistent with how the term is understood in other UNCITRAL texts on electronic commerce, making data “available” does not imply usability of the data, which is a matter of data conformity.⁴ Nor does it presuppose an entitlement to use the data, which is both a matter of data conformity and use rights.

34. Data availability is not a technical concept. The term “available” is intended to be technology neutral and does not presuppose any particular arrangement or technical means for accessing the data. The term “available” is intended to be given an autonomous meaning, consistent with article 4.

35. Paragraph 2 also states that the obligation to provide data comprises an obligation to provide “any information necessary to access the data”. [*To be completed based on the Working Group’s consideration of the issues identified in [A/CN.9/WG.IV/WP.192](#), paras. 17–19.*]

References

[A/CN.9/1162](#), paras. 73–78, 89; [A/CN.9/1197](#), paras. 33, 45, 51; [A/CN.9/1202](#), paras. 12–16; [A/CN.9/1241](#), paras. 41–44.

F. Article 6. Mode of provision of the data

36. Article 6 is inspired by article 31 of the CISG and deals with how the data is made available to the data recipient (i.e. the mode of provision).

1. Paragraph 1

37. Paragraph 1 obliges the data provider to provide the data by the agreed mode of provision. As noted above (para. 26), the agreement need not be manifested in the contract between the data provider and data recipient but may, for instance, be

⁴ See *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996* (United Nations publication, Sales No. [E.99.V.8](#)), para. 103 (discussing data availability in the context of article 15 of the MLEC).

manifested in their mutual assent to the rules of a data exchange operated by a third party that sets the conditions for the provision of data via the platform.

2. Paragraph 2

38. In the absence of any agreement, paragraph 2 obliges the data provider to provide the data by either of the two modes described in subparagraphs (a) and (b), namely (i) delivering the data to the data recipient, or (ii) giving the data recipient access to the data in a particular information system. Paragraph 2 does not prioritize either mode. While they are described in broad terms to reflect the main modes of provision in practice, paragraph 2 does not pretend that they are the only modes upon which the parties may agree under paragraph 1. The term “mode of provision” is intended to be technology neutral and encompasses new modes of providing data that may emerge over time.

39. Both modes of provision involve putting the data recipient in a position to use the data. The main difference between them is whether, as between the parties, the data is available for use in a system under the control of the data recipient or data provider.

(a) Delivery of data

40. The concept of “delivering” data in paragraph 2(a) encompasses delivery by electronic means or by handing over a physical object containing the data.

41. Consistent with other UNCITRAL texts on electronic commerce, data may be delivered by electronic means in a number of ways. The data provider may transmit the data from its information system to an information system of the data recipient, in which case the data would be delivered when it enters the information system of the data recipient. Data may also be delivered within the same information system. For instance, data may be delivered to an electronic address of the data recipient within the system, in which case the data would be delivered when it reaches that address. This is particularly relevant where the provision of data involves a third-party intermediary, such as a data exchange.

42. Paragraph 2(a) recognizes that delivery may be initiated by the data recipient exporting (or retrieving) the data from the data provider’s information system, which presupposes that the data provider has enabled that function. The data would thus be delivered when the data provider is able to export the data (i.e. it is capable of being retrieved). The term “export” is used instead of “port” as the focus is on the data leaving an information system, as well as to avoid any confusion with the concept of “portability”.

(b) Giving access to data

43. The concept of “access” encompasses the ability of the data recipient to read the data. In itself, “access” does not presuppose any particular use of the data, which is a matter for the use rights regime between the parties under article 9.

3. Paragraph 3

44. Paragraph 3 recognizes that, whichever mode is used, the data provider may need to take additional steps to put the data recipient in a position to use the data. [*To be completed based on the Working Group’s consideration of the issues identified in A/CN.9/WG.IV/WP.192, para. 21.*]

References

[A/CN.9/1132](#), paras. 27–28; [A/CN.9/1162](#), paras. 71–73, 78; [A/CN.9/1197](#), paras. 44–47; [A/CN.9/1202](#), paras. 17–24, 62; [A/CN.9/1241](#), paras. 45, 49–50, 54.

G. Article 7. Timing of provision of the data

45. Article 7 is inspired by article 33 of the CISG. It is intended to apply to a variety of data transactions, including the provision of data as a single occurrence, at recurring intervals (including by way of updates) or continuously. It is also intended to apply to the provision of data that is not in existence at the time of the conclusion of the contract, as in the case of data generated by a connected device.

46. The concept of “time frame” encompasses notions of periodicity (how often data is provided) and timeliness (how promptly data is provided once generated or otherwise comes into existence). Article 7 is thus concerned with dates and periods of time. However, it is not concerned with currency, which is a matter of data conformity. Accordingly, the provision of “real-time” data, which ordinarily assures a certain periodicity and timeliness of provision (i.e. data provided continuously and as soon as it is generated), as well as a certain currency of the data that is provided, potentially engages both articles 7 and 8. Article 7 is also not concerned with the duration of provision, which is a matter of data use under article 9.

47. The default rule in paragraph 2 requires the data to be provided “without undue delay”. This differs from article 33(c) of the CISG, which requires delivery “within a reasonable time after the conclusion of the contract”. The standard in paragraph 2 is designed to be more adapted to the peculiar attributes of data, particularly the speed at which it can be provided, and to accommodate different modes of provision. The point in time from which the delay is measured depends on the data transaction. For some transactions, it may be the conclusion of the contract (e.g. an existing dataset provided via a data exchange); for others, it might be the moment when the data is generated or otherwise comes into existence. Whether a delay is “undue” also depends on the transaction. For instance, a delay may be justifiable where the cause of the delay is ordinarily associated with the type of data provided or the mode of provision used (e.g. temporary service disruptions or interruptions in transmission).

References

[A/CN.9/1132](#), paras. 29–30; [A/CN.9/1197](#), paras. 49–50; [A/CN.9/1202](#), paras. 25–28; [A/CN.9/1241](#), paras. 56–59.

H. Article 8. Conformity of the data

1. Introduction

48. Article 8 deals with data conformity, which is essentially concerned with whether the data provided meets certain standards affecting its usability under the contract. It is inspired by the rules on conformity of goods that are set out in articles 35 to 44 of the CISG. It is based on an understanding that the essential components of conformity in the CISG are transposable to data with adaptations on account of the peculiar attributes of data. Data conformity can be closely connected with – and sometimes difficult to discern from – the mode and timing of provision, which are matters dealt with in articles 6 and 7, respectively. This is particularly the case for data that is provided at recurring intervals or continuously (e.g. in real-time).

2. Basic standard

49. Paragraph 1 establishes a basic rule that defers to the agreement of the parties as to the “quantity, quality and description” of data. As noted above (para. 26), the agreement need not be manifested in the contract between the data provider and data recipient but may, for instance, be manifested in their mutual assent to the rules of a data exchange operated by a third party that sets the conditions for the provision of data via the platform.

50. In the context of data, “quantity”, “quality” and “description” tend to overlap:

(a) “Quantity” refers, among other things, to the range of data elements covered by a dataset and thus encompasses characteristics such as data completeness. The quantity of data is connected to the periodicity of data provision (how often the data is provided), which engages article 7;

(b) “Quality” encompasses intrinsic characteristics such as accuracy and currency. As such, data quality is connected to the timeliness of the data provision, which also engages article 7. It also encompasses the concept of “traceability”, which incorporates assurances as to the authenticity (or origin) of the data and its integrity (whether the data remains unaltered);

(c) “Description” encompasses characteristics such as the format and structure of the data, as well as the level of granularity (how precise the values in a dataset are) and types of data that are to be included or excluded (e.g. personal data).

3. Supplementary standards

51. Paragraph 2 establishes a set of supplementary standards that apply unless otherwise agreed by the parties. While the standard in subparagraph (a) is applicable in all cases, the standards in subparagraphs (b) and (c) are stated to apply only in specific cases. Each of the standards is intended to be capable of objective determination:

(a) Subparagraph (a) is a modified form of the standard of fitness for ordinary purposes set out in article 35(2)(a) of the CISG. It acknowledges that the intended use of the data is not always apparent and that the fitness of the data can vary depending on the industry and role played by the data recipient in the data value chain;

(b) Subparagraph (b) establishes a standard of fitness for particular purposes that is modelled closely on article 35(2)(b) of the CISG; [*To be completed based on the Working Group’s consideration of the issues identified in A/CN.9/WG.IV/WP.192, para. 24.*]

(c) Subparagraph (c) is modelled closely on article 35(2)(c) of the CISG. The words “sample or model” encompass data previews. [*To be completed based on the Working Group’s consideration of the issues identified in A/CN.9/WG.IV/WP.192, paras. 25–26.*]

52. Paragraph 3 provides a basic assurance to the data recipient that the data is lawfully provided and can lawfully be used. While it distinguishes lawfulness of provision (addressed in subparagraph (a)) from lawfulness of use (addressed in subparagraph (b)), it may be that the same law renders both provision of the data by the data provider and use of the data by the data recipient unlawful. For remarks on the concept of “using” data, see below (paras. 64–66).

53. Together with articles 6 and 9, paragraph 3 operates to ensure that the data recipient is put in the position to use the data under the contract. It treats “lawfulness” as a matter of data conformity, which may differ from the approach taken in some legal systems. Paragraph 3 is cast as a stand-alone provision in recognition that it is not necessarily concerned with the characteristics of the data, but rather with the legal regimes that may impede the provision or use of the data under the contract. It also avoids giving the impression that the application or enforcement of those legal regimes are subject to agreement of the parties (compared, for instance, to the chapeau of article 8(2)).

54. Paragraph 3(a) is primarily concerned with compliance with regulatory laws, such as laws on data privacy and protection, whose application is preserved by article 2(4). It therefore effectively puts compliance with those laws on an additional contractual footing.

55. Paragraph 3(b) is formulated in terms similar to article 42(1) of the CISG in that it refers (i) to the provision of data “free from any right or claim of a third party” and

(ii) to those rights and claims of which the data provider “knew or could not have been aware”. However, the scope of rights and claims covered by paragraph 3(b) is different from article 42(1) of the CISG. Paragraph 3(b) is concerned with the rights and claims that are encompassed by the concept of “data rights” [*explanation to be included in the introduction section (see para. 2)*], which encompasses a broader range of rights and claims than those envisaged in article 42(1). Moreover, it is stated to apply only to those rights and claims that “impede” the use of the data. Accordingly, it does not require the data to be completely unencumbered; the provision of data that is encumbered by a “data right” would comply with paragraph 3(b) where the data provider obtained the third-party permissions or consents that are required in order for the data recipient lawfully to use the data as contemplated in the contract and under article 9. [*To be completed based on the Working Group’s consideration of the issues identified in A/CN.9/WG.IV/WP.192, paras. 27–29.*]

4. Assessing data conformity

56. Paragraph 4 provides guidance on assessing data conformity.

57. Paragraph 4(a) contains an indicative, non-exhaustive list of core characteristics of data that may be considered when applying the standards set out in paragraphs 1 to 3. It does not require all of the of listed characteristics to be considered, nor does it assign priority to any of them. Consistent with the principle of technology neutrality, the characteristics listed in paragraph 4(a) do not presume the use of any particular method to maintain data conformity, which will depend on the data transaction. The “integrity” of the data encompasses the provision of data free from malicious software that may alter or delete the data.

58. Paragraph 4(b) acknowledges the relevance of industry standards in assessing data conformity, where they exist and are applicable. The term “industry standards”, which is used in other UNCITRAL texts on electronic commerce, refers to a broad concept that covers not only normative instruments of varying binding nature, such as codes of conduct, but also trade usages and custom. It is not limited to technical specifications. Industry standards can play an important role in increasing data access and sharing, thereby helping to close data divides, and in ensuring interoperability of different information systems that process the data.

59. Paragraph 4(b) also recognizes the practice in some industries and for some types of data transactions of the parties agreeing on procedures for assessing the conformity of the data and remedying any lack thereof.

60. While primarily aimed at the conformity standards in paragraphs 1 and 2, the chapeau of paragraph 4 indicates that it might also be relevant to the requirements in paragraph 3. This does not imply, however, that the application or enforcement of the legal regimes captured by paragraph 3 is subject to the agreement between the parties or applicable industry standards.

References

[A/CN.9/1093](#), paras. 87, 90; [A/CN.9/1132](#), paras. 33–37, 42–46; [A/CN.9/1162](#), paras. 77, 81–83, 85; [A/CN.9/1197](#), paras. 52–60, 70–71; [A/CN.9/1202](#), paras. 30–47; [A/CN.9/1241](#), paras. 60–69.

I. Article 9. Use of the data

1. Establishing a contractual regime for the use of data

61. Article 9 establishes a basic regime for the rights and obligations of the parties with respect to the use of the data provided under the contract. It is premised on the assumption that data is not generally recognized as an object of property rights and that, in the absence of a comprehensive property-like regime for data rights, contracts for the provision of data remain an important source of law regulating the use of data.

62. Consistent with this approach, article 9 avoids terminology associated with “sales” or “licences”. It therefore makes no reference to either of the parties “owning” the provided data (or any derived data, which is addressed in article 10) or to the data provider “licensing” the data to the data recipient. While some of the rights listed in paragraph 1 might be said to reflect a “sales” approach, others might be said to reflect a “licence” approach. Article 9 is not intended to favour either approach. Moreover, the basic regime that it establishes applies regardless of the mode of provision, even though in practice the different modes described in article 6(1) might be associated with different rights regimes.

63. Article 9 is complemented by the basic regime for derived data, which is established by article 10.

2. The concept of “using” data

64. Paragraph 4 is intended to clarify the meaning of “using” data in technical terms. The reference to performing “operations” recognizes the connection between “using” data and the concept of “processing” data. While article 10 refers to “processing” data, the choice to refer to “using” data in article 9 acknowledges that that terminology is more widely used in practice, even though “processing” may be a more commonly used legal concept.

65. Definitions of “processing” in domestic and international legal texts, particularly those on data privacy and protection, commonly contain a non-exhaustive list of operations that may be performed on data, such as generating, collecting, recording, organizing, structuring, altering, storing, retrieving, transmitting and erasing data. Depending on the context, one or more of these operations may be involved in “using” data or in “providing”, “accessing”, “sharing” or “transferring” data. In the context of article 10, operations such as combining and aggregating may be involved in the generation of derived data.

66. The term “using” data is intended to be broad and covers operations performed by the data recipient within its own information system as well as operations involved in the onward provision of that data to a third party. In the context of article 9, “using” data would not involve generating data as the data already exists. It would not involve operations involved in “providing” the data to a third party, whether by sharing or transferring the data, or by disclosing the information represented by the data.

3. Paragraph 1

67. Paragraph 1 allocates use rights between the data provider and data recipient. It establishes default rules on the scope, duration and exclusivity of the rights of the data provider and the residual rights of the data provider. As with the conformity standards in article 8(2), the allocation of rights in paragraph 1 applies unless otherwise agreed by the parties. It follows that, if the contract is silent, and in the absence of any other agreement (e.g. their mutual assent to the rules of a data exchange), the use rights allocated in paragraph 1 apply. For the avoidance of doubt, it is worth specifying that, by recognizing that the parties may depart from the default right of the data recipient under subparagraph (a) to use the data “for any lawful purpose”, paragraph 1 does not recognize that the parties may agree for the data recipient to use the data for unlawful purposes. Rather, it recognizes that the parties may agree for the data recipient to use the data only for specified purposes.

68. Paragraph 1 is concerned with the legal relationship between the data provider and data recipient and therefore the allocation of rights applies only as between them. Paragraph 1 is not intended to affect the legal relationship between either of the parties and third parties. It follows that the data recipient cannot invoke rights allocated under paragraph 1 to deny a third-party right or claim that impedes the use of the data (a matter addressed in article 8(3)(b)). Similarly, the data recipient cannot rely on rights allocated under paragraph 1 to avoid limitations imposed by law on the scope or duration of use of the data, including restrictions under data privacy and protection

laws on the purposes for which the data may be used (a matter addressed in article 2(4)).

69. Paragraph 1(a) recognizes that the scope of data rights is essentially a matter of the purposes and means of data processing. Under the default rule, the scope of the right of the data recipient to use the data is unlimited; the data recipient is entitled to use the data for any purpose and by any means. In some legal systems, the data recipient would be said to be in control of the data. The term “purpose”, which is also used in article 8(2)(a), is primarily concerned with economic purposes, which will vary depending on the industry and role played by the data recipient in the data value chain. The term “means” is used in a technical sense, referring to the methods and technologies that are used to process the data, including the choice of systems and software. In practice, where the data provider gives the data recipient access to the data in the data provider’s system, it may also provide the means to use the data (e.g. an online platform for processing the data). In such a case, the contract can be expected to depart from the default rule in paragraph 1(a).

70. Paragraph 1(b) is concerned with the duration of use. Under the default rule, the data recipient has the right to use the data for an unlimited period of time (i.e. in perpetuity). In practice, where the data provider provides the means to use the data (see para. 69 above), the duration of use will ordinarily be tied to the duration of access to the platform. In such a case, the contract can be expected to depart from the default rule in paragraph 1(b).

71. Paragraph 1(c) is concerned with the onward provision of the data. Depending on the roles played by the parties in the data value chain, the onward provision of data can be critical to generating value from the data, yet it can also compromise the economic position of the data provider. Under the default rule, the data recipient has no right to provide the data to a third party. This rule favours the data provider who, in the absence of a comprehensive property-like regime for data rights, must rely on contractual measures to control the downstream processing of the data it provides.

72. Paragraph 1(c) effectively restricts the right of the data recipient to use the data and places the burden on the data recipient to lift the restriction. In practice, it is common for third-party service providers to hold the data on behalf of the data recipient. Third-party associates may also be engaged in the joint exploitation of the data. In such cases, the contract can be expected to depart from the default rule in paragraph 1(c) by specifying the purposes for which the data recipient may provide the data to the third parties. In transactions reflecting a “sales” approach, the contract can be expected to depart from the default rule entirely (i.e. no restrictions on the onward provision of the data).

73. Paragraphs 1(d) and (e) are concerned with the exclusivity of use. They recognize that, owing to the non-rivalrousness of data, the data provider need not give up pre-existing data rights when providing data to the data recipient. Under the default rule, the data provider retains the right to use the data and to provide it to third parties, thereby qualifying the right allocated to the data recipient under paragraph 1(a) as non-exclusive. The reference to the data provider “continuing” to use the data signifies that paragraph 1(d) is about preserving pre-existing rights, not establishing new rights.

4. Paragraph 2

74. *[To be inserted if article 9(2) is retained: see [A/CN.9/WG.IV/WP.192](#), paras. 34–35].*

5. Paragraph 3

75. *[To be inserted if article 9(3) is retained: see [A/CN.9/WG.IV/WP.192](#), para. 36].*

References

[A/CN.9/1132](#), paras. 38–45, 84–85; [A/CN.9/1197](#), paras. 62–63; [A/CN.9/1202](#), paras. 48–66; [A/CN.9/1241](#), paras. 68–73.

J. Article 10. Derived data

76. Article 10 deals with the data that the data recipient generates – or “derives” – by using the data provided by the data provider under article 9 (sometimes referred to as the “source data”). Derived data is a new product of the data recipient’s own economic activity which contributes additional insights and extracts new value. The inclusion of a specific provision dealing with derived data recognizes the economic importance of derived data as well as the potential for legal uncertainty when the rights of the parties in derived data are not addressed contractually.

77. Paragraph 1 establishes a default rule by which the data recipient has the right to provide derived data to a third party. This rule stands in contrast to the default rule in article 9(1)(c), which restricts the onward provision of the source data. Paragraph 1 does not allocate use rights in derived data between the parties. For the data recipient, the right to use the derived data does not derive from the contract but rather from the lawful use of the source data and other data with which it is processed. For the data provider, it is assumed that use rights (if any) would be addressed in the arrangement under which the derived data is provided to the data provider as a data recipient (e.g. a data pooling arrangement). For completeness, it is worth recalling that the text does not address data rights outside the contractual setting, such as intellectual property rights.

78. The definition of “derived data” in paragraph 2 requires the data to be “sufficiently distinct” from the source data. This requirement is designed to avoid article 10 circumventing the use rights regime under article 9, in particular the protection of the economic position of the data provider provided by article 9(1)(c). It also reflects what gives derived data its value.

79. Paragraph 2 contains an indicative, non-exhaustive list of circumstances that may be considered when applying the requirement. The list demonstrates that intrinsic values (e.g. the content and structure of the derived data) as well as extrinsic values (e.g. the economic activity of the data recipient in generating the derived data) may be relevant. The requirement is not intended to be met merely by anonymizing or aggregating personal data comprising the source data.

References

[A/CN.9/1132](#), paras. 47–50; [A/CN.9/1162](#), para. 86; [A/CN.9/1197](#), paras. 64–66; [A/CN.9/1202](#), paras. 67–71.

K. Article 11. Common obligations of the data provider and data recipient

80. [To be inserted based on the Working Group’s consideration of the issues identified in [A/CN.9/WG.IV/WP.192](#), para. 39–40.]

L. Article 12. Non-performance

81. [To be inserted based on the Working Group’s consideration of the issues identified in [A/CN.9/WG.IV/WP.192](#), para. 41–46.]

M. Article 13. Passive provision of data

82. [To be inserted based on the Working Group's previous deliberations (A/CN.9/1197, paras. 47–48, 61, 72; A/CN.9/1202, paras. 21–23, 78–79; A/CN.9/1241, paras. 10–21, 46–53) and its consideration of the issues identified in A/CN.9/WG.IV/WP.192, paras. 47–57.]

ADVANCE COPY