United Nations A/CN.9/WG.IV/WP.183

General Assembly

Distr.: Limited
23 August 2023

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-sixth session
Vienna, 16–20 October 2023

Default rules for data provision contracts (first revision)

Note by the Secretariat

Contents

		Page
I.	About this note	2
II.	Revised draft rules	2
	A. Introduction	2
	B. Rules on general matters	2
	C. Rules on mode of provision	7
	D. Rules on conformity of data	9
	E. Rules on the use of data	11
	F. Rules on derived data	15
	G. Rules on remedies	15

V.23-16276 (E)

I. About this note

1. This note sets out a revised set of default rules for data provision contracts for consideration by the Working Group at its sixty-sixth session. It has been prepared by the secretariat to incorporate the deliberations and decisions of the Working Group in its consideration of an initial draft presented to the sixty-fifth session (A/CN.9/1132, paras. 9–51).

II. Revised draft rules

A. Introduction

2. At its sixty-fifth session, the Working Group commenced work on the topic of data contracts under the mandate given by the Commission at its fifty-fifth session, following earlier preliminary discussions on the topic at its sixty-third session (A/CN.9/1093, paras. 77–95). Work proceeded on the basis of an initial draft set of default rules for data provision contracts ("initial draft") that had been prepared by the secretariat (A/CN.9/WG.IV/WP.180, chapter III, sections B to E), which was accompanied by a glossary of terms (ibid., chapter II) and an introduction of the concept of "default rules" (ibid., chapter III, section A). After a first reading of the draft, the Working Group agreed that the secretariat should prepare a revised set of default rules for consideration at its sixty-sixth session (see A/CN.9/1132, para. 92).

3. The revised set of default rules set out in this note are accompanied by remarks which explain the origin and intent of the rules. The remarks also highlight issues on which the Working Group may wish to focus at its sixty-sixth session, which include:

(a) Accommodating data pooling arrangements (articles 2 and 5) and mixed contracts (article 2);

(b) Developing rules on the use of data upon expiration of the term or earlier termination of the contract (article 8);

(c) Developing rules for the use of data made available in a system controlled by the data provider (article 8);

(d) Expanding the rules on rights in derived data (article 9) and remedies (article 10).

4. Consistent with views expressed at the sixty-fifth session, the revised set of default rules are drafted as provisions which could eventually take the form of model legislation or model contract clauses (A/CN.9/1132, para. 13). If the rules were to take the form of model contract clauses, the rules on general matters set out in the next section would presumably be transposed into an accompanying legal guide on the use of the model clauses.

5. In considering the revised set of default rules, the Working Group may wish to bear in mind the broader policy objectives that data provision contracts engage, including those pursued by a range of other international initiatives on data governance and cross-border data flows, as previously reported to the Working Group (A/CN.9/WG.IV/WP.180, chapter IV).

B. Rules on general matters

Article 1. Definitions

For the purpose of these rules:

(a) "Data" is a representation of information in electronic form;

(b) "Using" data includes performing one or more operations on data, and extends to accessing, sharing, porting, transferring or providing data.

Remarks on article 1

1. Introduction

6. Article 1 is new. It draws on the glossary of terms presented to the Working Group[1] which was discussed at its sixty-fifth session (A/CN.9/1132, paras. 18–23 and 25).

2. The concept of "data"

7. The definition of "data" in paragraph (a) is broad (A/CN.9/1132, para. 18). Confining the scope of data and data provision contracts to which the rules apply is left to article 2.

8. The concept of data as a representation of information underlies the concept of "data message" in UNCITRAL texts on electronic commerce, which is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means" (i.e. other than by paper-based means).[2] Earlier UNCITRAL texts on electronic commerce – such as the Model Law on Electronic Commerce (MLEC) and the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) were primarily concerned with data as a communication between the parties (hence "data message"). Conversely, these rules are concerned with data as a commodity, regardless of what the information represented by the data communicates.[3] Accordingly, the term "data" is used.

9. The reference to "electronic form" in the definition of "data" implies the quality of machine-readability, and thus suitability for automated processing (A/CN.9/1132, para. 22). It encompasses data in digital form (i.e. information represented by a string of "zeros" and "ones"), which is currently the focus of trade in data (ibid., para. 20). 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) (ibid., para. 21).

3. The concept of "using" data

10. Paragraph (b) clarifies what it means to "use" data, reflecting the deliberations within the Working Group regarding the relationship between "processing" and "using" data (A/CN.9/1132, para. 25). In effect, paragraph (b) reflects the broad technical definition of "processing" data but uses the terminology of "using" data to reflect common usage. "Porting" data refers to the operation by which the data recipient initiates a transfer of data from the data provider under a data provision contract (A/CN.9/1093, para. 83) and is therefore particularly relevant where data is provided under article 5(1)(b).

Article 2. Scope of application

(1) These rules apply to contracts for the provision of data under which one party (the "data provider") provides data to another party (the "data recipient").

(2) These rules do not apply to data comprising:

(a) Software;

(b) Electronic transferable records;

(c) The result of electronic identification or the result deriving from the use of a trust service.

---

[1] See A/CN.9/WG.IV/WP.180, para. 4.

[2] See, e.g. UNCITRAL Model Law on Electronic Commerce, art. 2(a); United Nations Convention on the Use of Electronic Communications in International Contracts, art. 4(c).

[3] For completeness, it is worth recalling that the term "data message" in UNCITRAL texts is not limited to communication but is also intended to encompass computer-generated records that are not meant for communication, and therefore comprises "electronic records": see A/CN.9/WG.IV/WP.176, para. 13.

(3) These rules do not apply to contracts in which the preponderant part of the obligations of the data provider consists in the supply of services with respect to the data;

(4) Nothing in these rules affects the application to data provision contracts of any law related to data privacy and protection, the protection of consumers, trade secrets or intellectual property[, or any laws governing transactions in specific electronic records].

Remarks on article 2

1. Introduction

11. Article 2 is new and implements several suggestions made during the sixty-fifth session of the Working Group about the scope of application of the rules (A/CN.9/1132, paras. 19 and 24).

12. Data commonly traded under data provision contracts is data that is generated and used in commercial activity (e.g. research and development, production, distribution and consumption of goods and services). This data is sometimes referred to as "industrial data", although the term has not yet acquired an established legal meaning.

13. Data provision contracts are typified by transactions in "big data" (A/CN.9/1132), a term which generally refers to large volumes of data that are collected from a variety of sources and generated and processed at high velocity (the so-called "3 Vs" of volume, velocity and variety). A similar assumption underpins the Principles for a Data Economy, jointly developed by the American Law Institute and European Law Institute (hereafter the "ALI/ELI Principles"), whose primary focus is on "records of large quantities of information as an asset, resource or tradable commodity".[4] Difficulties in identifying the limits of "big data" make it an unsuitable reference point for defining the scope of application of the rules. Article 2 therefore employs other methods to pinpoint the types of contracts to which the rules apply.

2. The concept of "data provision contracts"

14. Paragraph 1 of article 2 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.

15. Paragraph 1 states that the rules apply to contracts "for" the provision of data, and thus to contracts the subject of which is the provision of data. Accordingly, a contract would not be a "data provision contract" merely because it contained information sharing obligations that could be performed by electronic means (A/CN.9/1132, para. 19). In this sense, paragraph 1 is complemented by paragraph 3 (discussed in para. 22 below).

16. Applying the rules to contracts "for" the provision of data raises the question as to how the rules should apply to mixed contracts that involve the supply of goods, such as goods fitted with sensors that provide the recipient with data on their operation (assuming that the data provision component is incorporated into the contract). One option would be to allow for the residual application of the rules, i.e. the rules would apply to the extent that the provision of data is not governed by other law (e.g. sale of goods law). Paragraph 4 of article 2 (discussed in para. 25 below) could be expanded to preserve the application of such other laws.

17. The concept of data provision contracts reflected in paragraph 1 is consistent with contracts under which the parties provide data to each other (e.g. a two-way data sharing arrangement).[5] Under such contracts, each party would act as a "data provider" and "data recipient", and the default rules would apply accordingly,

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

[5] See A/CN.9/WG.IV/WP.180, para. 15.

depending on the data concerned. On a related matter, it is worth mentioning that no default rule has yet been considered on the price for provided data.

18. Data provision contracts may thus cover certain "data pooling" arrangements, under which the parties provide data to a shared "data pool". Some data pools are comprised of data in an information system (e.g. part of an online platform) controlled jointly by the parties or by a third-party service provider, in which case the contract may exhibit traits of a "data processing contract" and therefore be caught by the exclusion in paragraph 3 (see para. 22 below). Other pools may simply be comprised of data provided individually by each party, whether via access to an information system controlled by that party of otherwise (i.e. a two-way data-sharing arrangement). At the sixty-fifth session, some support was expressed within the Working Group for including data pooling contracts within the scope of work (A/CN.9/1132, para. 19). The Working Group may wish to consider how data pooling arrangements should be covered in the rules, bearing in mind paragraph 3.

19. The concept of data provision contracts is also consistent with contracts under which data is provided through a third-party intermediary via an online platform (A/CN.9/1132, para. 19 and 27). In that case, the intermediary would not be party to the contract, but would likely have separate data-processing contracts in place with the data provider or the data recipient (or both).[6] See further discussion under rule 5 on accommodating the use of third-party intermediaries in the provision of data.

3. Exclusion of software and other data products

20. Broad support has been expressed within the Working Group to exclude software from scope (A/CN.9/1132, para. 19). This is reflected in subparagraph (a) of paragraph 2. Contracts for the supply of software are already an established type of contract in many jurisdictions, and the rules are not intended to displace the legal regimes that apply to such contracts.

21. In a similar vein, the rules are not intended to apply to dealings in electronic records that are governed by special substantive law regimes, such as electronic transferable records within the meaning of the UNCITRAL Model Law on Electronic Transferable Records (MLETR) (A/CN.9/1132, para. 87), or other particular types of digital assets (ibid., para. 19). Subparagraph (b) of paragraph 2 has been inserted to clarify that transactions involving electronic transferable records are excluded from scope. The Working Group may wish to consider whether it is necessary or desirable to list other types of electronic records (as that term is defined in the MLETR), or whether it would be sufficient to expand paragraph 4 (as indicated by the text in square brackets) so as to preserve those special substantive law regimes. Arguably, these dealings already fall outside the scope of the rules by virtue of the definition of "data" in article 1 as they are not concerned with the "information" that data represents, but rather with the functions that it delivers (e.g. a computer program) or the rights and obligations that it represents (e.g. cryptocurrency) (ibid., para. 19).

4. Exclusion of "data-processing contracts" and other contracts

22. Paragraph 3 draws on the wording of article 3(2) of the United Nations Convention on Contracts for the International Sale of Goods (CISG). The words "with respect to the data" have been added to clarify that the exclusion is intended to cover contracts under which one party provides data processing services for another party (i.e. "data-processing contracts"). Contracts for data scraping, cloud-based services, data analytics and electronic transmission services would ordinarily be caught by this paragraph.[7] Under data-processing contracts, the service recipient provides data to the service provider for processing and the service provider provides processed data to

[6] This is based on the contractual structure of online platforms previously described by the secretariat: see A/CN.9/1117, para. 25.

[7] See A/CN.9/WG.IV/WP.180, para. 18.

the service recipient. Neither instance would be regarded as the provision of data for the purposes of these rules.

23. Paragraph 3 would also encompass contracts for the supply of services via the Internet or other communications network by electronic means. This may raise questions as to the characterization of contracts under which data is made available for consumption through an online platform.

24. The Working Group may wish to consider whether the exclusion strikes an appropriate balance, recalling that the distinction between data provision contracts and data processing contracts is not always clear-cut,[8] and mindful of references at the sixty-fifth session to certain modes of providing data as "services" (see A/CN.9/1132, para. 29).

5. Preserving other laws

25. Paragraph 4 is modelled on article 2(4) of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) and is intended primarily to preserve the application of laws and regulations on data privacy and intellectual property (A/CN.9/1132, paras. 24 and 34). By virtue of paragraph 4, the rules avoid the impracticality – if not impossibility – of limiting their application to the provision of data that does not comprise personal data, while ensuring that protective and regulatory measures regarding personal data continue to apply with full force. They also avoid the need to exclude from scope data that is subject to intellectual property rights. Where personal data or intellectual property rights are involved, the default rules do not seek to regulate the measures that the parties are to take to comply with the particular requirements of personal data and intellectual property law. If any of the default rules need to be varied to accommodate the particular arrangement between the parties as to the exploitation of intellectual property rights or processing of personal data, this can be done under article 3.

26. Paragraph 4 is also intended to preserve the application of special laws on consumer protection. The Working Group may wish to consider whether this approach sufficient to address the issue of consumer contracts (A/CN.9/1132, para. 24), or whether an express exclusion (e.g. modelled on article 2(a) of the CISG) should be included in the rules.

Article 3. Party autonomy

(1) The parties may derogate from or vary by agreement any of these rules.

(2) Such an agreement does not affect the rights of any person that is not a party to that agreement.

Remarks on article 3

1. Introduction

27. Article 3 is new and implements a suggestion made during the sixty-fifth session of the Working Group (A/CN.9/1132, para. 14). The new rule is intended to address some of the uncertainty expressed during the sixty-fifth session surrounding the concept of "default rules" (ibid., paras. 10 and 14).

2. Party autonomy

28. Party autonomy is a fundamental principle underpinning commercial law and UNCITRAL texts that 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 MLETR. Like with other UNCITRAL texts, article 3 recognizes party autonomy within the limits of mandatory law (see article 2(4)) and without affecting rights and obligations of third parties (article 3(2)).

[8] Ibid., para. 20.

Article 4. Interpretation

(1) In the interpretation of these rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith in international trade.

(2) Questions concerning matters governed by these rules which are not expressly settled therein are to be settled in conformity with the general principles on which they are based.

Remarks on article 4

1. Introduction

29. Article 4 is new and picks up a suggestion made during the sixty-fifth session of the Working Group (A/CN.9/1132, para. 37). It is based on a provision found in many UNCITRAL texts, including the CISG and texts on electronic commerce.

2. Guiding principles

30. Some of the principles that have informed the development of the rules, and which may therefore be relevant for applying paragraph 2, include the understanding that data provision contracts do not fall into any established type of contract (A/CN.9/1132, para. 39), and an acknowledgment that the peculiar qualities of data as intangible and non-rivalrous can affect the commercial relationships and transactions involving data (A/CN.9/1132, para. 16). As the secretariat has previously observed:[9]

(a) Data provision contracts tend to be more relational, in the sense that they involve the provision of data as part of an ongoing relationship;

(b) The intangibility of data and its suitability for automated processing mean that real-time or continuous provision is particularly important. Similarly, data can be provided via an information system that also limits its use;

(c) The non-rivalrousness of data means that the data provider does not necessarily need to give up its pre-existing rights in the data, and thus may provide the same data to third parties. In other words, multiple data recipients can exploit the same data contemporaneously;

(d) The absence of a comprehensive property-like regime for data rights means that contractual rights are relied upon to secure the use of data;

(e) Data is not always provided in exchange for payment.

31. It has also been acknowledged within the Working Group that the availability of copied data means that data can be resupplied in the event of loss, damage or lack of conformity (A/CN.9/1132, para. 51).

C. Rules on mode of provision

Article 5. Mode of provision

(1) The data is provided by:

(a) Delivering the data to an information system designated by the data recipient;

(b) Making the data available to the data recipient or to a person designated by data recipient in an information system under the control of the data provider.

(2) The data provider and data recipient shall cooperate with each other where such cooperation could reasonably be expected with respect to the mode of provision

[9] Ibid., para. 24.

of the data under the contract, including technical, organizational and security measures.

(3) Without limiting paragraph 2, the data provider and data recipient shall notify each other of any data breach affecting the provision of the data within a reasonable time after becoming aware of the data breach.

Remarks on article 5

1. Introduction

32. Rule 5 is based on the rules set out in paragraph 28 of the initial draft, which have been revised to reflect the suggestions made within the Working Group during the sixty-fifth session (A/CN.9/1132, paras. 27–28).

2. Different modes of providing data

33. Paragraph 1 contemplates the provision of data by transmission and access, which constitute the two main modes of provision in practice (A/CN.9/1132, para. 28). Other modes of provision can be provided for by agreement of the parties under article 3.

34. Paragraph 1 has been further revised to refer to the data being "delivered" rather than "transmitted". This is designed to align the rule with the understanding of risk allocation that emerged at the sixty-fifth session (A/CN.9/1132, para. 31). In line with the approach taken in article 20 of the MLIT, the concept of "delivering" data is intended to coincide with the receipt of data (i.e. entry into the information system designated by the data recipient).[10]

35. The term "information system" is borrowed from the MLEC, where it is defined to mean "a system for generating, sending, receiving, storing or otherwise processing data messages". The term is employed in provisions of the MLEC on the dispatch and receipt of data messages exchanged between parties, where it is "intended to cover the entire range of technical means used for transmitting, receiving and storing information".[11] Similarly, article 5 borrows from the MLEC the concept of a system being under the "control" of a party.

36. Paragraph 1 is intended to accommodate modes of provision involving a third-party service provider, even if the rules themselves are not concerned with the contractual relationship between that service provider and the parties to the data provision contract. Specifically, the information system designated by the data recipient for delivery, or the information system used to access the data, may be operated by a third-party "data intermediary" (e.g. via an online platform) on behalf of either party.

3. Cooperation on technical, organizational and security measures

37. The rule on security requirements (rule 2(b) in paragraph 28 of the initial draft) has been replaced with the rule in paragraph 2, which establishes an obligation of the parties to cooperate. The new rule picks up on a suggestion made during the sixty-fifth session (A/CN.9/1132, para. 28).

[10] *UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services* (United Nations publication, Sales No. E.23.V.10), para. 216.

[11] See, e.g. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996* (United Nations publication, Sales No. E.99.V.8), para. 40.

4. Notification of data breaches

38. Paragraph 3 is new and establishes an obligation to notify data breaches as an application of the obligation to cooperate. It is inspired by articles 7 and 14(2) of the MLIT. Consistent with the MLIT, the concept of "data breach" refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or unauthorized access to, data transmitted, stored, or otherwise processed. By virtue of article 2(4), paragraph 3 does not displace any similar obligation imposed under data privacy and protection legislation or other law.

Article 6. Timing of provision

The data shall be provided according to the timeframe fixed by or determinable from the contract or otherwise without undue delay.

Remarks on article 6

1. Introduction

39. Article 6 is inspired by article 33 of the CISG (time of delivery of goods) and has been adapted to data. It is based on the rule set out in paragraph 30 of the initial draft, which has been revised to reflect the suggestions made within the Working Group at its sixty-fifth session (A/CN.9/1132, paras. 29–30).

2. Periodicity of provision

40. It has been observed within the Working Group that data may be provided either as a single occurrence, at recurring intervals, or continuously (A/CN.9/1132, para. 29). Article 6 is intended to accommodate each of those cases.

3. Timeliness vs. currency

41. The words "within a reasonable time" have been replaced with the words "without undue delay" to accommodate issues with interruption of data supply (A/CN.9/1132, para. 30). Article 6 is not concerned with the currency of data provided, which is a matter of conformity of data that is addressed in article 7 (see A/CN.9/1132, para. 29).

D. Rules on conformity of data

Article 7. Conformity of data

(1) The data shall be of the quantity, quality and description required by the contract.

(2) The data conforms with the contract if:

(a) It is fit for any particular purpose expressly or impliedly made known to the data provider at the time of the conclusion of the contract, except where the circumstances show that the data recipient did not rely, or that it was unreasonable for the data recipient to rely, on the data provider's skill and judgment;

(b) It possesses the qualities of data which the data provider has held out to the data recipient as a sample or model;

(c) It possesses the qualities of data in accordance with any representations that the data provider makes with respect to the data; and

(d) It is provided lawfully.

(3) In assessing whether the data conforms with the contract, regard is to be had to:

(a) All relevant characteristics of the data, including its authenticity, integrity, completeness, accuracy and currency, as well as the format and structure of the data; and

(b) Any agreement between the parties or applicable industry standards.

(4) The data recipient shall notify the data provider of any lack of conformity of the data within a reasonable time after discovering it.

(5) Without limiting the previous paragraphs, [where the contract provides for the provision of data over a period of time,] the data provider and data recipient shall cooperate with each other on matters related to the conformity of data, including establishing requirements for the quantity, quality and description of the data, for the examination of data, and for remedying any lack of conformity.

Remarks on article 7

1. Introduction

42. Article 7 is inspired by the rules on conformity of goods in article 35 of the CISG. It is based on the rules set out in paragraph 36 of the initial draft, which have been revised to reflect the proposals put forward within the Working Group at its sixty-fifth session (A/CN.9/1132, paras. 33–37).

2. Elements of data conformity

43. The primary test of conformity in paragraph 1 defers to the terms of the contracts as to the "quantity, quality and description" of data. While these elements are drawn from the CISG with respect to goods, they can readily be transposed and adapted to data.

44. Paragraph 3 provides guidance on assessing data conformity. It lists some of the elements of data conformity that were put forward during the sixty-fifth session (A/CN.9/1132, paras. 33 and 35). It also confirms the relevance of industry standards in assessing data conformity, where they exist and are applicable (see A/CN.9/1132, para. 37). The Working Group may wish to consider how else industry standards (including codes of conduct) may be relevant in the performance of data provision contracts.

45. The concepts of "quantity", "quality" and "description" tend to overlap when applied to data. In addition to the elements listed in paragraph 3 (i.e. authenticity, integrity, completeness, accuracy and currency), they cover elements such as format and level of granularity of the data, as well as the type of data (e.g. by reference to the person or object to which the data relates, or to the data being anonymized so as not to relate to an identified or identifiable person) and source of the data (e.g. the identification of the data source). Paragraph 1 serves as a reminder for the parties to pay special attention to defining the data provided under the contract.

46. Subparagraph (a) of paragraph 2 retains the rule in the initial draft requiring data to be fit for particular purposes. However, the rule in the initial draft that required the data to be fit for ordinary purposes has not been retained on the basis that such a rule is not suitable for data (A/CN.9/1132, para. 36). Subparagraph (b) of paragraph 2 retains the reference to "sample or model" on the assumption that those words encompass data previews (A/CN.9/1132, para. 35).

47. Subparagraph (c) of paragraph 2 is new and reflects the suggestion for data quality to be assessed by reference to public statements by the data provider (A/CN.9/1132, para. 35). The wording draws on articles 6(b) and 14(1)(b) of the MLIT.

48. Subparagraph (d) of paragraph 2 reflects the view that "lawfulness" of the data is an element of data conformity (A/CN.9/1132, para. 34). The rule is concerned with the lawfulness of provision by the data provider (e.g. that providing the data under the contract does not infringe any applicable law) and not with the lawfulness of use by

the data recipient, which is addressed in article 8 (see A/CN.9/1093, para. 90). This approach may differ from the approach taken in domestic law. For instance, pursuant to the Digital Content and Digital Services Directive of the European Union, the law of EU member States treats any limitation on the use by the consumer of "digital content" (i.e. defined as data in digital form) resulting from a violation of third-party rights, in particular intellectual property rights, as a matter of conformity. [12] Conversely, the ALI/ELI Principles treat lawfulness of use as separate to conformity.

3. Notification of non-conformity

49. Paragraph 4 is new and contains a basic obligation on the data recipient to notify the data provider of any lack of conformity. During the sixty-fifth session, doubts were raised about the desirability of adapting the rules on detecting and notifying lack of conformity in articles 34 to 40 of the CISG to data (A/CN.9/1132, para. 37). In particular, it was noted that the timeframe for examining goods (i.e. "within as short a period as is practicable in the circumstances") was not suitable for data, for which conformity was usually detected not at the time the data was available, but at the time the data was used. The rules set out in paragraph 37 of the initial draft have therefore not been retained.

4. Cooperation on matters of data conformity

50. Paragraph 5 is new and responds to observations made within the Working Group about assessing data conformity in practice, particularly where data is provided over a period of time (A/CN.9/1132, para. 37).

51. Paragraph 5 builds on article 4(1), which already points to the observance of good faith in the performance of contractual obligation relating to data conformity. The wording of the paragraph is inspired by article 5.1.3 of the 2016 UNIDROIT Principles of International Commercial Contract. An express obligation to cooperate in matters of conformity could be regarded as a departure from the type of commercial relationship that underlies contracts for the sale of goods (as foreshadowed in para. 30 above). Yet in substance, the outcome might not differ from the type of regime codified in articles 34 to 40 of the CISG, which effectively mandates some degree of cooperation between the parties to examine the goods and remedy (or cure) any lack of conformity.

52. Paragraph 5 applies "where the contract provides for the provision of data over a period of time". Those words have been inserted in square brackets to invite the Working Group to consider whether this approach is appropriate. Recalling the observation within the Working Group as to the periodicity of data provision (see para. 40 above), the obligation to cooperate would apply to the provision of data at recurring intervals or continuously. [13]

E. Rules on the use of data

Article 8. Use of provided data

(1) As between the parties to the contract:

(a) The data recipient is entitled to use the data for any lawful purpose and by any lawful means[, subject to any agreed limitations];

[12] See Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *Official Journal of the European Union*, L 136 (22 May 2019), p. 1.

[13] It is worth noting that the periodicity of data provision is relevant to conformity under the Digital Content and Digital Services Directive of the EU (discussed in para. 48 above), where the rules on conformity depend on whether the digital content (or digital services) are supplied "continuously over a period of time" or as a "single act of supply or a series of individual acts of supply".

(b) The data provider is entitled to continue using the data, including by providing it to third parties.

(2) The data provider and data recipient shall cooperate with each other where such cooperation could reasonably be expected with respect to the use of the data under the contract.

(3) Without limiting paragraph 2:

(a) The data provider shall ensure that the data recipient is in a position lawfully to use the data [for the purpose or by the means specified in the contract];

(b) The data provider shall notify the data recipient of any legal requirement with respect to the use of the data by the data recipient for the purpose or by the means specified in the contract without delay after becoming aware of the requirement;

(c) The data recipient shall ensure that the data is not used in a manner that infringes the rights of the data provider or of a third party with respect to the use of the data;

(d) The data recipient shall notify the data provider of any legal requirement with respect to the use of the data under the contract without delay after becoming aware of the requirement, unless it is reasonable to expect the data provider to have been aware of the requirement.

(4) In this rule, "legal requirement" includes a legal right or claim.

Remarks on article 8

1. Introduction

53. Article 8 is based on the rules set out in paragraph 44 of the initial draft, which have been revised to reflect the suggestions made within the Working Group during the sixty-fifth session (A/CN.9/1132, paras. 38–46).

2. Establishing a contractual framework for the use of data

54. Article 8 establishes a basic framework 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 peculiar qualities of data that distinguish data provision contracts from contracts for the sale of goods. Owing to the nature of "goods" as an object of property rights, as well as the characteristics of a "sale" as a transaction involving the transfer of ownership, the CISG does not contain provisions on how the buyer is to use the goods. Beyond requiring the seller to "transfer the property in the goods", the CISG leaves it to the law of property and other legal regimes to govern the use of the goods. Conversely, data is generally not recognized as an object of property rights (see A/CN.9/1117, para. 47) and is therefore not amenable to ownership nor to the rights that the law attributes to ownership. Given the absence of a comprehensive property-like regime for data rights, (ibid., para. 46), data provision contracts remain the primary source of law regulating the use of data.

55. In keeping with the deliberations of the Working Group at its sixty-fifth session, article 8 avoids the concepts of "sale" or "licence" (A/CN.9/1132, para. 39). Accordingly, it makes no reference to the ownership of the provided data (or of any derived data, which is addressed in article 9) or to the data provider "licensing" the data to the data recipient.

3. Rights of the parties

56. Paragraph 1 of article 8, which lays down the basic rights of the parties with respect to the use of the data, reproduces rule 1 in paragraph 44 of the initial draft with the revisions suggested within the Working Group at its sixty-fifth session (A/CN.9/1132, para. 40). The Working Group may wish to consider whether the rule

in subparagraph (a) should make special provision for contracts under which the data is made available to the data recipient in an information system under the control of the data provider, which may be designed to limit how the data recipient can use the data (as contemplated in article 5(1)(b)), including by preventing the data from being ported from the system. For instance, under the ALI/ELI Principles, the data recipient is only entitled to port data when it "can reasonably be expected in a transaction of the relevant kind"; however, the porting of derived data (see rule 9 below) is not so limited. The words "subject to any agreed limitations" have been inserted in square brackets as a starting point for consideration.

57. An issue raised, but not deliberated, at the sixty-fifth session is the duration of use of the data (A/CN.9/1132, para. 39). The Working Group may wish to consider developing a default rule on the use of data upon expiration of the term or earlier termination of the contract. Again, it may be appropriate to make specific provision for contracts under which the data is provided by accessing an information system under the control of the data provider (see para. 56 above).

4. Cooperation on matters relating to data use

58. At the sixty-fifth session, broad support was expressed for establishing an obligation of the parties to cooperate in performing the contract (A/CN.9/1132, para. 43). Paragraph 2 of article 8 establishes such an obligation, which replaces rules 2 and 3 in paragraph 44 of the initial draft. Like article 7(5) (see para. 51 above), the wording of paragraph 2 is inspired by article 5.1.3 of the 2016 UNIDROIT Principles of International Commercial Contract.

5. Mutuality of obligations of the parties

59. Paragraph 3 of article 8 establishes a series of obligations which are intended to reflect a mutuality of obligations between the data provider and data recipient (A/CN.9/1132, paras. 41–45).

60. Each obligation in paragraph 3 is formulated as an application of the obligation to cooperate in paragraph 2 (see A/CN.9/1132, para. 45). It is suggested that each obligation could therefore be subjected to an assessment of what "could reasonably be expected" of the party on which the obligation is imposed. This approach could overcome the potentially unreasonable results arising from imposing obligations on either party without any limitation, particularly in terms of geographic scope (recalling that, at the sixty-fifth session, doubts were raised about the desirability and feasibility of confining obligations on the data provider by reference to the place where the data is used or the place where the data recipient has its place of business: ibid., para. 46). The Working Group may wish to consider whether this approach is appropriate.

61. The obligation in subparagraph (a) effectively recasts the warranty in the first sentence of rule 3 in paragraph 44 of the initial draft as an obligation on the data provider to remove impediments to the data recipient using the data. The new formulation seeks to clarify that the rule is concerned with the lawfulness of the use of data by the data recipient and not with the lawfulness of the provision by the data provider, which is addressed in article 7. It promotes the view, expressed within the Working Group at its sixty-third session, that the data recipient should have an assurance that the data can lawfully be used under the contract (A/CN.9/1093, para. 90). It does not use the wording of articles 41 and 42 of the CISG (which refer to the delivery of goods "free from any right or claim of a third party") to emphasize that the obligation is not a matter of conformity of the data provided, but rather of ensuring that the data recipient can exercise its rights to use the data under the contract.

62. It was noted during the sixty-fifth session that the ALI/ELI Principles establish more onerous obligations on the data provider with respect to the use of the data by the data recipient, and it was suggested that that project might provide guidance to the Working Group (A/CN.9/1132, para. 43). To that end, the Working Group may wish

to note that the ALI/ELI Principles establishes two obligations on the data provider (referred to as the "supplier") with respect to the use of the data by the data recipient:

(a) First, an obligation to place the data recipient in the position of having a legal right, effective against third parties, that is sufficient to result in the data recipient's "control" of the data and the right to engage in such other "data activities" of which the data provider had notice and in which it could reasonably expect to engage;

(b) Second, an obligation to place the data recipient in a position, at the time the data is provided, of being able rightfully to engage in those activities.[14]

63. While the first obligation is aimed at ensuring that the data recipient has adequate intellectual property rights to use the data, the second obligation is aimed at ensuring that there are no legal impediments to using the data at the time of provision, including under the law relating to trade secrets, data privacy and database rights.

64. Compared to the obligations established by the ALI/ELI Principles, the obligation in subparagraph (a) of paragraph 3 is limited by reference to the purpose or the means specified in the contract, as well as an assessment of what "could reasonably be expected" of the data recipient (as discussed in para. 60 above). Consistent with the deliberations at the sixty-fifth session (A/CN.9/1132, para. 40(a)), it also avoids the term "control".

65. Subparagraphs (b) and (d) implement a suggestion to impose an obligation on each party to notify the other party of any right or claim affecting the data (A/CN.9/1132, para. 45). The concept of "legal requirement" is understood broadly to encompass not only compliance with mandatory law (e.g. data privacy and protection legislation), but also non-interference with the "data rights" of the other party and of third parties. This is clarified by paragraph 4 of article 8. The concept of "data rights" has previously been described by the secretariat in the following terms (A/CN.9/1117, paras. 27–28):

> The notion of "data rights" (or "rights in data") is not yet firmly established in legal doctrine and can be interpreted differently in different contexts. In a commercial law context, the term may be defined loosely as any of a variety of rights, claims and remedies that afford a person (the rightholder) control over data, including the manner in which data is processed, the purposes for which it is provided, and the outcome of that processing.
>
> […]
>
> Data rights, as defined, are already recognized under a range of laws, including laws relating to trade secrets, data privacy and database rights. In broad terms, those existing regimes afford a range of controls over how data is processed, including (i) gaining access to data, (ii) requiring a person to desist from processing data, and (iii) requiring data to be corrected or erased.

66. The obligation in subparagraph (c) picks up on suggestions made during the sixty-fifth session to impose obligations on the data recipient with respect to the use of the data under the contract, including an obligation to prevent downstream abuse of data (A/CN.9/1132, para. 41), and an obligation to comply with rights and claims notified by the data provider (ibid., para. 42).

[14] The concept of "control" of data is defined in the ALI/ELI Principles to mean "being in a position to access the data and determine the purposes and means of its processing", while "data activities" is defined to mean "activities by a person with respect to data, such as collection, acquisition, control, processing and other activities including onward supply of data".

F. Rules on derived data

Article 9. Derived data

As between the parties to the contract:

(a) The data recipient is entitled to determine the purposes and means of using any data ("derived data") that it generates by using the data under paragraph 1 of article 8;

(b) The data provider is entitled to use the derived data as agreed by the parties.

Remarks on article 9

1. Introduction

67. Article 9 reproduces the text of the proposal put forward at the sixty-fifth session as a basis for further consideration (A/CN.9/1132, paras. 48–49) with some modifications to align with revisions made to other rules.

2. The concept and importance of "derived data"

68. At the sixty-fifth session of the Working Group, some support was expressed for including default rules on the rights of the parties in derived data, noting the economic importance of derived data, as well as the legal uncertainty regarding the rights of the parties in derived data when the issue is not addressed in the contract (A/CN.9/1132, para. 47).

69. Paragraph (a) of article 9 establishes a straightforward definition of "derived data" that is consistent with the term used in other legislative and non-legislative projects on data transactions. For the data recipient, rights in derived data will likely be an important issue where the data is provided under article 5(1)(b) and the data recipient processes the data using the information system controlled by the data provider. For the data provider, rights in derived data will likely be an important issue where the data is provided under a data pooling arrangement.

70. The Working Group may wish to consider the parameters of "derived data" as defined in paragraph (a). One issue is whether it includes metadata generated by the system controlled by the data provider if the data is provided under article 5(1)(b), the generation of which would presumably be attributed to the data provider (although it may be regarded as being "co-generated" by the data recipient).[15] Another issue is whether derived data needs to be sufficiently distinct in the sense of being processed by such industrial activity as to no longer be linked to the provided data.

G. Rules on remedies

Article 10. Remedies

(1) If the data provider fails to provide the data in accordance with article 5 and 6, the data recipient may require the data provider to do so.

(2) If the data provider is entitled by law to claim restitution from the data recipient of data provided under the contract, that requirement may be met by the data provider erasing the data from any information system under its control, provided that the data provider remains in a position to use the data.

(3) Nothing in these rules affects the application of any rule of law or agreement of the parties that may govern the legal consequences of a failure of a party

[15] Such data may be likened to "cloud service-derived data" as defined in *Notes on the Main Issues of Cloud Computing Contracts* (United Nations publication, 2019).

to comply with its obligations under the contract other than as provided for in this rule.

Remarks on article 10

71. At its sixty-fifth session, the Working Group heard a preliminary exchange of views on default rules on remedies for breach (A/CN.9/1132, para. 51). On the one hand, it was observed that existing laws on remedies for breach of contract applied to data provision contracts, and that an obligation to pay damages could be applied without difficulty. On the other hand, it was observed that the peculiar qualities of data might require some other remedies to be adapted, such as an obligation to make restitution or specific performance. Some support was expressed to consider developing default rules on those other remedies.

72. Article 10 is new and is presented to the Working Group as a basis for further deliberations on the issue of remedies.

73. Paragraph 1 addresses the remedy of requiring performance (i.e. "specific performance" as it is known in some jurisdictions) in the event of a failure by the data provider to provide the data. It applies to the obligations of the data provider to provide the data under articles 5 (mode of provision) and 6 (timing of provision). As for conformity of the data (article 7), article 10 defers to the arrangements between the parties under article 7(5), which provides for the parties to cooperate in remedying any lack of conformity. The Working Group may wish to consider supplementing that provision with specific obligations on the part of the data provider to remedy the lack of conformity. Article 10 makes no special provision for remedies in the event of a failure by either party to comply with its obligations under article 8 (use of provided data). The Working Group may wish to consider whether it is desirable to include a rule similar to article 12(1) and 24(1) of the MLIT regarding liability for loss caused to a party due to a failure by the other party to comply with those obligations.

74. Article 81(2) of the CISG recognises the remedy of restitution, and ordinarily applies to require the buyer to return goods delivered under the contract in the event of default by the buyer. Given the peculiar qualities of data, the function of restitution as a remedy against the data recipient may be served not by the data recipient returning data provided under the contract, but rather by the erasing the data from its systems. Paragraph 2 establishes a basic rule that reflects this approach.

75. Paragraph 3 reflects the view (referred to in para. 71 above) that existing laws on remedies for breach of contract apply to data provision contracts. The Working Group may wish to consider whether other existing remedies for breach would benefit from default rules that transpose their application to data.