United Nations A/CN.9/WG.IV/WP.188

General Assembly

Distr.: Limited
20 January 2025

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-eighth session
New York, 24–28 March 2025

Default rules for data provision contracts (third revision)

Note by the Secretariat

Contents

V.25-00752 (E)

I. Introduction

1. The annex to this note contains an annotated third revision of the draft default rules for data provision contracts, which the secretariat has prepared to reflect the deliberations of the Working Group at its sixty-seventh session (Vienna, 18–22 November 2024) (A/CN.9/1197, paras. 29–72).

2. When, at that session, the Working Group considered the next steps in the project, the need to maintain a "coherent approach" in the rules was emphasized, particularly as regards the treatment of the "passive" provision of data. With this in mind, and as the sixty-eighth session will be the first session of the Working Group devoted entirely to data provision contracts, this note offers some remarks to take stock of the project and to identify issues that the Working Group may wish to consider at the session.

II. Taking stock of the project

A. Background to the current mandate

3. At its fifty-fifth session, in 2022, the Commission agreed to mandate the Working Group to proceed with work on data provision contracts on the basis of preparatory work documented in a proposal contained in a note submitted by the secretariat (A/CN.9/1117).[1] That preparatory work comprised work carried out by the secretariat on data transactions, stemming from a mandate given by the Commission at its fifty-first session,[2] as well as preliminary discussions of the nature and scope of possible future work on data transactions that took place at the sixty-third session of the Working Group (A/CN.9/1093, chapter VI). The note emphasized the central role played by contract law in data transactions and the potential for harmonized rules to facilitate an enabling environment for cross-border data flows (A/CN.9/1117, paras. 28–30). It explained that gaps exist not only in terms of the application of contract law principles to data contracts, but also in terms of the provisions to be contained in data contracts.

B. Development of default rules

4. No decision has been taken on the form and legal nature of the eventual output of the project. At the fifty-fifth session, the Commission heard that several options had been canvassed in the preliminary discussions within the Working Group, including the development of "default rules" to be included in a legislative text, a guide to good practice for parties and a legislative guide.[3] The Working Group has worked on the basis of a draft set of default rules, which have been prepared and revised by the secretariat,[4] on the understanding that the rules establish standards that the parties are able to vary, or from which they are able to derogate, based on the principle of party autonomy (A/CN.9/1132, para. 14). It has been suggested that the rules should be calibrated bearing in mind which party ought to bear the burden of departing from the default setting (A/CN.9/1197, para. 62).

5. Default rules do not presuppose a particular final form of instrument, and the Working Group has acknowledged that the rules could eventually take the form of a

[1] *Official Records of the General Assembly*, *Seventy-seventh Session, Supplement No. 17* (A/77/17), para. 163.

[2] Ibid, *Seventy-third Session, Supplement No. 17* (A/73/17), para. 253(b).

[3] Ibid., para. 164.

[4] An "initial draft" (A/CN.9/WG.IV/WP.180) was considered at the sixty-fifth session (A/CN.9/1132, paras. 9–51), a "first revision" (A/CN.9/WG.IV/WP.183) was considered at the sixty-sixth session (A/CN.9/1162, paras. 59–89) and a "second revision" (A/CN.9/WG.IV/WP.186) was considered at the sixty-seventh session (A/CN.9/1197, paras. 29–72).

legislative text or a contractual text (A/CN.9/1132, paras. 10 and 13). The final form of the instrument will nevertheless affect how the rules are formulated, as well as their content (for instance, rules on scope of application, party autonomy and interpretation will not be as relevant to model contract clauses).

6. The United Nations Convention on Contracts for the International Sale of Goods (CISG) has served as a reference point for identifying the legal issues to be addressed in the default rules (A/CN.9/1132, para. 16). Nonetheless, the Working Group has cautioned the need to be sensitive to the differences between the sale of goods and data transactions, including the peculiar qualities of data as intangible and non-rivalrous, and the different commercial practices and relationships involved (ibid.).[5] It has also observed that data provision contracts do not fall into any established type of contract (ibid., para. 39), and that the data provider will not always be "in the business" of providing data (ibid., para. 45). The Working Group has avoided referring to data provision contracts in terms of "sales" or "licences" so as to focus on the rights and obligations of the parties (ibid., para. 39).

7. The secretariat has highlighted some of the different features of data transactions that may guide the content of the default rules, including (i) the intangibility of data and its suitability for automated processing mean that real-time or continuous provision is particularly important, (ii) 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 (i.e. copies of the data) to third parties, (iii) the availability of copied data means that data can be resupplied in the event of loss, damage or lack of conformity, (iv) the absence of a comprehensive property-like regime for data rights means that contractual rights are relied upon to secure the use of data, and (v) data is not always provided in exchange for payment of a price.[6]

8. The result is a set of default rules on the rights and obligations of the parties to data provision contracts that are organized according to particular legal issues that arise, rather than according to the obligations of the parties (compare Part Three of the CISG). Notably, the default rules establish a basic regime regarding the use of the data provided under the contract,[7] as well as the treatment of derived data. The default rules do not address contract formation, but do address remedies (i.e. rights and obligations of the parties in the event of non-performance).

9. The default rules are intended to cover a variety of different "types" of data provision contracts, including contracts under which data is provided in exchange for data (e.g. a decentralized data pool), contracts under which data is provided through a third-party intermediary (e.g. a centralized data pool or other data exchange), and contacts under which data is provided as a one-off delivery, at regular intervals (e.g. whenever updates are available) or continuously (e.g. data generated by a connected device). At the same time, the default rules acknowledge that differential treatment of data provision contracts may be warranted depending on which party retains "control" of the data.

C. Other initiatives

10. It was recommended at the fifty-fifth session of the Commission that work be mindful of the output of other legislative and non-legislative projects, and the Working Group has been apprised of potential intersections with other international initiatives on data governance and cross-border data flows.[8] A recent example is the

[5] The Working Group has also avoided deliberating questions as to whether data provision contracts can be characterized as a "contract for sale" or whether data can be characterized as "goods" for the purposes of the CISG (A/CN.9/1132, para. 17).

[6] A/CN.9/WG.IV/WP.183, paras. 30–31.

[7] As explained in remarks on earlier versions of the draft rules, because data is not universally recognized as an object of property rights, data provision contracts remain the primary source of law regulating the use of data (A/CN.9/WG.IV/WP.186, para. 40).

[8] See A/CN.9/WG.IV/WP.180, paras. 47–51.

Global Digital Compact, contained in annex I to the Pact for the Future that was adopted by the General Assembly on 22 September 2024, which sets out a range of commitments that potentially engage data provision contracts, particularly in pursuit of the objective to advance responsible, equitable and interoperable data governance approaches. At the sixty-seventh session, it was recognized that data interoperability engaged issues of data conformity under data provision contracts (A/CN.9/1197, para. 59).

III. Issues for consideration

A. The "passive" provision of data

1. Introduction

11. At the sixty-seventh session, the Working Group considered the application of the default rules to transactions where a person merely authorizes another person to access data. The example was given of a person who deploys a connected device authorizing another person to access data generated by the device. Specifically, a question arose as to whether the default rules apply only where the data provider performs an active role in the flow of data, or whether they also apply where it performs a "passive" role (A/CN.9/1197, para. 33). While the passive provision of data (by a data subject) is of particular concern in the context of data privacy and protection, it was acknowledged that such transactions do arise in a business-to-business context involving non-personal data flows. It was noted that the passive provision of data is accommodated by the Principles for a Data Economy, jointly developed by the American Law Institute and European Law Institute (hereafter the "ALI/ELI Principles"), which establish a special set of default terms for "contracts for authorization to access" (ibid., para. 46).

12. Broad support was expressed within the Working Group to accommodate the passive provision of data within the draft rules (A/CN.9/1197, para. 33). At the same time, it was acknowledged that the rules should apply differentially with a view to limiting the responsibility of a data provider which plays a passive role (ibid., para. 39). The rules on conformity, use and remedies were singled out in particular (ibid., paras. 54, 57, 61 and 68). It was also cautioned that accommodating the passive provision of data should not result in excessively complex rules (ibid., para. 61).

2. Do the default rules apply?

13. Applying the default rules to the passive provision of data raises several issues regarding the scope of application of the rules, some of which were already touched on at the sixty-seventh session. The Working Group may wish to elaborate on these issues at the sixty-eighth session.

(a) The data for which authorization to access is given could be held by a third party (e.g. a third party providing support services relating to the connected device). In this transaction, the person giving authorization would presumably be the "data provider" for the purposes of the default rules if the data is held on their behalf.

(b) The person could give authorization without the existence of a contract. The person would only be a "data provider" if a contract exists with the person to whom authorization is given, even if it is one that merely provides for that authorization to be given (A/CN.9/1197, para. 46). At the sixty-sixth session, a concern was expressed within the Working Group about characterizing a person as a "data provider" merely because they consented to the collection and further processing of data (ibid., para. 40).

(c) The person could give authorization as a condition (or as counter-performance) for acquiring the connected device or for receiving support services provided by the other person. In the second revision, the secretariat suggested that the term "contracts for the provision of data" implies that the default rules are concerned

with contracts whose object is the provision of data, which recalls a suggestion within the Working Group for work to focus on contracts characterized by the provision of data (A/CN.9/1162, para. 68), as well as a concern about capturing contracts merely because of incidental information sharing obligations that are capable of being performed by electronic means (A/CN.9/1132, para. 18). Accordingly, a contract for the sale or licensing of goods or for the provision of services, under which data is provided by the buyer or licensee, is unlikely to be a "contract for the provision of data".

3. How should the default rules apply?

14. Assuming that contracts for the passive provision of data can fall within the scope of application of the default rules, additional questions arise as to how to sufficiently identify these contracts, and whether a given default rule should apply to those contracts with modifications or should be disapplied altogether. The Working Group may wish to elaborate on these issues at the sixty-eighth session.

15. One approach, suggested at the sixty-seventh session, is to identify contracts for the passive provision of data by reference to the "mode of provision". Specifically, it was suggested that a third mode of provision could be prescribed (in article 6), namely "giving the data recipient authorization to access the data through its own means" (A/CN.9/1197, para. 48). It was observed that this mode might overlap with the mode of provision that is already listed in paragraph 6(b), given that a connected device could be a component of an "information system". Additionally, the line between "giving […] authorization to access the data" and "making the data available" might not be so clear.

16. Another approach, suggested at the sixty-seventh session, is to refer to the "role" played by the data provider with respect to the data (A/CN.9/1197, para. 33). It was observed that the data provider would have no control over what data was generated by the connected device or the circumstances in which that data was accessed by the data recipient. A similar view emerges from the ALI/ELI Principles, which acknowledge "the passive nature of the authorizing party's anticipated conduct under the contract and the authorizing party's lack of meaningful influence on the transaction". Principle 10 provides that the special set of default terms established for "contracts for authorization to access" apply if, in view of those circumstances, the authorizing party "cannot reasonably be expected" to undertake responsibilities under the default terms established for the other types of data provision contracts. Testing what a party could or could not be reasonably expected to do is not unfamiliar to UNCITRAL texts (including the CISG), and is already reflected in some of the default rules.

17. An alternative test, which is also not unfamiliar to UNCITRAL texts as a basis for differentiating the legal effects of transactions, is whether the transaction was within the party's "ordinary course of business", which picks up the observation (mentioned in para. 6 above) that the data provider will not always be "in the business" of providing data.[9] This test might offer greater legal certainty, but it would also cover some contracts for the "active" provision of data.

B. Remedies

18. At the sixty-sixth session, the Working Group heard some general observations about the rights and remedies available to a party in the event of non-performance by the other party. It was observed that monetary damages could be applied without difficulty to data transactions (A/CN.9/1132, para. 51), which suggests that it might be more readily available as a remedy for breach of data provision contracts as compared to sales contracts under the CISG. It was also observed that remedies (and

[9] See, e.g. art. 34 of the UNCITRAL Model Law on Secured Transactions and article 2(8) of the UNCITRAL-UNIDROIT Model Law on Warehouse Receipts.

the circumstances in which they are available) might need to be adapted on account of the peculiar qualities of data, in particular its non-rivalrousness (ibid.). This would appear to be particularly relevant to remedies for lack of conformity and termination (avoidance). For instance, non-conform data might be readily cured by updating or resupplying the data, and data might be readily erased by the data recipient upon termination.

19. At the sixty-seventh session, different views were expressed about remedies (A/CN.9/1197, paras. 68–70). On one view, it was sufficient to preserve remedies under applicable law (e.g. for breach of contract). On another view, the default rules should contain a comprehensive yet non-exhaustive list of remedies, including termination (avoidance), price reduction and compensation, which would be available not only for non-provision of the data under articles 6 and 7 (mode and timing of provision of the data), but also lack of conformity under article 8 and non-performance of other obligations. It was generally recognized that the default rules (now in article 12) do not deal with judicial remedies but rather with the rights and obligations of the parties in the event of non-performance.

20. At the sixty-eighth session, the Working Group may wish to continue its consideration of the issue, in particular:

(a) Whether – and in what circumstances – the non-defaulting party should have the right to monetary damages, to withhold performance or to terminate (avoid) the contract; and

(b) Whether other rights should be recognized to address non-performance of obligations under article 9 (use of the data), such as a right to require the defaulting party to refrain from using the data.

C. Other issues

21. Other issues that the Working Group may wish to consider are highlighted in the notes accompanying the third revision, in particular:

(a) Including a definition of “information system” (note 12);

(b) Elaborating the concept of “access” to data (note 23);

(c) Including a requirement for the data provider to provide information necessary to access the data (note 24);

(d) Revising the standard of fitness for ordinary purposes in article 8(2)(a) (note 30);

(e) Revisiting the obligations of the data recipient regarding the use of the data (note 37);

(f) Distinguishing derived data from data provided under the contract (note 45).

Annex

Article 1. Definitions[10]

For the purpose of these rules:

(a) "Data" means a representation of information in electronic form or other form suitable for processing[11] in an information system;[12]

(b) "Using" data includes performing one or more operations involved in the processing of data, such as sharing, porting, transferring or providing data.[13]

Article 2. Scope of application[14]

1. These rules apply to contracts for the provision of data under which one party (the "data provider") provides data [that it holds][15] to another party (the "data recipient"), whether or not with the involvement of a third party.[16]

2. These rules do not apply to contracts for the supply of software.[17]

---

[10] *Definitions – general*: Article 1 draws on a glossary of terms that was considered by the Working Group at its sixty-fifth session (A/CN.9/1132, paras. 18–23 and 25). It has been revised to reflect the suggestions made at its sixty-sixth session (A/CN.9/1162, paras. 88–89) and sixty-seventh session (A/CN.9/1197, paras. 31–33).

[11] *Definition of "data" – suitability for automated processing*: At the sixty-seventh session, it was indicated that machine readability could be understood not only as a matter of defining data (i.e. that the data be suitable for processing by a computer), but also as a matter of data conformity (i.e. that the data be in a particular format, such as to allow the information to be extracted using commonly available software applications) (A/CN.9/1197, para. 32). To avoid ambiguity, the definition of "data" has been revised to replace "machine readable form" with "form suitable for processing in an information system". The revised definition mirrors definitions in other international instruments, including the recently adopted United Nations Convention against Cybercrime (A/RES/79/243, annex).

[12] *Concept of "information system"*: The term "information system", which is also used in article 6, is borrowed from the UNCITRAL Model Law on Electronic Commerce (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. The Working Group may wish to consider inserting a definition of the term along these lines.

[13] *Concept of "using" data*: At the sixty-seventh session, there was broad agreement that the concept of "using" data as described in paragraph (b) provided a useful working definition (A/CN.9/1197, para. 31). The paragraph has been revised to clarify the relationship between "using" and "processing" data, which was touched on at the sixty-seventh session in the context of derived data (ibid., para. 64).

[14] *Scope of application – general*: Article 2 was inserted in the first revision following discussions at the sixty-fifth session (A/CN.9/1132, paras. 19 and 24). It has been revised to reflect the deliberations at the sixty-sixth session (A/CN.9/1162, paras. 62–70) and sixty-seventh session (A/CN.9/1197, paras. 34–41). Additional questions regarding the application of article 2 to contracts for the "passive" provision of data are discussed in the cover note (see para. 13).

[15] *Scope of application – requirement for the data provider to "hold" the data*: At the sixty-sixth session, it was suggested that the concept of "providing" data should be further elaborated (A/CN.9/1197, para. 33). The Working Group may wish to consider including the words in square brackets to clarify that the concept of "providing" data presupposes that the data provider holds the data that it provides (see also para. 14 of the cover note). Broad support has been expressed within the Working Group to avoid using the term "control" (e.g. when referring to a person "having control" or "controlling" data) (A/CN.9/1132, para. 40(a)). The secretariat suggests that the concept of "holding" should be understood in a neutral sense as referring to data that is in an information system under the control of the data provider, whether or not with the involvement of a third party.

[16] *Scope of application – contracts for the provision of data*: Paragraph 1 is discussed in the second revision (see A/CN.9/WG.IV/WP.186, paras. 9–21). It has been revised to remove the square brackets around the words "whether or not with the involvement of a third party" to reflect the deliberations at the sixty-seventh session (A/CN.9/1197, para. 34).

[17] *Scope of application – exclusion of contracts for the supply of software*: Paragraph 2 has been revised to reflect the deliberations at the sixty-seventh session (A/CN.9/1197, paras. 35–36).

[3. These rules do not apply to contracts concluded [by a data provider] for personal, family or household purposes[, unless the data provider, at any time before or at the conclusion of the contract, neither knew nor ought to have known that the data recipient was acting for any such purposes].][18]

4. Nothing in these rules affects the application of any rule of law that may govern the provision of data, including laws related to data privacy and protection, the protection of consumers, trade secrets or intellectual property.[19]

Article 3. Party autonomy[20]

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.

Article 4. Interpretation[21]

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.

Article 5. Obligation to provide the data[22]

1. The data provider shall provide the data to the data recipient as required by the contract and these rules.

---

[18] *Scope of application – exclusion of consumer contracts*: Paragraph 3 was inserted in the second revision to implement the prevailing view at the sixty-sixth session to exclude consumer contracts from the scope of the rules (A/CN.9/1162, para. 70). At the sixty-seventh session, there was broad support for the view that it was premature for the Working Group to take a decision on the issue. Paragraph 3 has been revised to reflect the options put forward at the session (A/CN.9/1197, paras. 39–40). Depending on the option preferred, the Working Group may wish to revisit the qualification in the second set of square brackets, which is discussed in the second revision (A/CN.9/WG.IV/WP.186, para. 22).

[19] *Scope of application – preserving other laws*: Paragraph 4 was inserted in the first revision and has been revised to reflect the deliberations at the sixty-sixth session (A/CN.9/1162, para. 70) and sixty-seventh session (A/CN.9/1197, paras. 39 and 41). In particular, the paragraph has been reformulated to reinsert the reference to laws related to "the protection of consumers" and to cover other mandatory laws.

[20] *Party autonomy – general*: Article 3 was inserted in the first revision. It was discussed at the sixty-seventh session (A/CN.9/1197, para. 42) and remains unchanged from the second revision.

[21] *Interpretation – general*: Article 4 was inserted in the first revision. It was discussed at the sixty-seventh session (A/CN.9/1197, para. 43) and remains unchanged from the second revision. It was suggested at that session that additional guidance was needed as to the "general principles" referred to in paragraph 2. Unlike recent texts prepared by the Working Group on electronic transactions, which are based on the fundamental principles of non-discrimination and technology neutrality, the default rules have been informed by general principles of contract law, including party autonomy, good faith and fair dealing. These general principles are distinct from the basic concepts and principles that have guided the development of the default rules, including those outlined in the cover note (para. 7).

[22] *Obligation to provide the data – general*: Article 5 reproduces article 5(1) of the second revision. As a stand-alone provision, it clarifies the intention to establish a general obligation of the data provider to provide the data, regardless of the mode by which the data is provided (A/CN.9/1162, para. 73). Article 5(2) of the second revision is retained in article 6 (see note 25).

2. The obligation of the data provider in paragraph 1 consists of giving the data recipient access[23] to the data[, including any information necessary to access the data[24]].

Article 6. Mode of provision of the data[25]

The data provider shall give the data recipient access to the data by the mode agreed upon by the parties, including by:

(a) Delivering the data to an information system outside the control of the data provider that is designated by the data recipient; or

(b) Making the data available to the data recipient in an information system under the control of the data provider.[26]

[23] *Obligation to provide the data – giving "access" to the data*: At the sixty-sixth session, it was observed that the essential component of the data provider's obligation to provide data is to make the data "accessible" to the data recipient (A/CN.9/1162, para. 73). It was suggested to include a definition of "access" (ibid., para. 89). The second revision thus stated that the data provider discharged its obligation to provide the data by "giving the data recipient access to the data" and suggested that, as the term "access" was only used in article 5, it might be sufficient to define the term in explanatory material. At the sixty-seventh session, it was suggested that the concept of "accessing" data under article 5 might need to be further elaborated. The Working Group may wish to consider the meaning of the term "access" as discussed in the second revision (A/CN.9/WG.IV/WP.186, paras. 28–29) and whether article 5(2) should be supplemented to reflect that discussion (e.g. by expressly requiring the data recipient to be put in the position to use the data under the contract).

[24] *Obligation to provide the data – information needed to access the data*: At the sixty-seventh session, the Working Group considered a question as to whether an obligation to give "access" to data that was encrypted included an obligation to deliver the encryption key. The text in square brackets, which is inspired by the reference to documents relating to goods sold in articles 30 and 34 of the CISG, has been included for the consideration of the Working Group as a possible way to address the question. In doing so, the Working Group may wish to consider the interplay with the obligation of the data provider to provide the data recipient with the means necessary to use the data in article 9(2)(a) (see note 41 below). The need to supply accompanying information is recognized in the OECD Recommendation of the Council on Enhancing Access to and Sharing of Data (2021), document C/MIN(2021)20/FINAL, which refers to the provision of data "together with any required meta-data, documentation, data models and algorithms" in a transparent and timely manner, as well as in the ALI/ELI Principles, which refer to the "inclusion of metadata, domain tables, and other specifications required for data utilization". In the ALI/ELI Principles, the presence of this information is a matter of data conformity.

[25] *Mode of provision of the data – general*: Article 6 reproduces article 5(2) of the second revision. The chapeau has been revised to reflect a suggestion supported at the sixty-seventh session to clarify that the mode is to be agreed upon by the parties and not determined unilaterally by the data provider (A/CN.9/1197, para. 48).

[26] *Mode of provision of the data – control vs designation of information systems*: The first revision referred to delivering the data to an information system "designated" by the data recipient, and to making data available in an information system "under the control" of the data provider, as the two "main" modes of provision in practice. This terminology was borrowed from article 15 of the MLEC. In the second revision, it was suggested to refer to the information system "designated" by the relevant party, while at the sixty-seventh session, it was noted that the designation of information systems was less meaningful than control thereof (A/CN.9/1197, para. 47). The Working Group may wish to revert to the terminology in the first revision with additional wording to paragraph (a) to accommodate data pooling arrangements in which the information system is under the joint control of both parties (see A/CN.9/WG.IV/WP.183, para. 18) and the data would thus be provided under paragraph (b) and not paragraph (a). Consistent with article 10 of the United Nations Convention on the Use of Electronic Communications in International Contracts, an information system under the control of the data provider is understood to encompass an "electronic address" designated by the data recipient within that system.

Article 7. Timing of provision of the data[27]

1. The data provider shall provide the data according to the time frame fixed by or determinable from the contract.

2. If no time frame is fixed by or determinable from the contract, the data provider shall provide the data:

(a) if the data is available to the data provider at the time of the conclusion of the contract, without undue delay;

(b) in all other cases, as soon as practicable after the data is available to the data provider.

Article 8. Conformity of the data[28]

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

2. In addition, the data shall:[29]

(a) [Be fit for the purposes for which data of the same description would ordinarily be used][Possess the characteristics that may reasonably be expected of data provided by the data provider in the circumstances];[30]

---

[27] *Timing of provision of the data – general*: Article 7 reproduces article 6 of the second revision, which in turn was based on a rule set out in the initial draft. It has been revised to reflect suggestions made at the sixty-fifth session (A/CN.9/1132, para. 29) and sixty-seventh session (A/CN.9/1197, para. 50). In particular, subparagraph 2(b) is designed to cover so-called "future data", whether it is provided at recurring intervals (e.g. whenever an update is available) or continuously (e.g. whenever a connected device generates data), or indeed whether the data needs to be generated or collected by the data provider according to the data recipient's specifications (a case described at the sixty-seventh session: ibid., para. 62). The term "practicable" is drawn from other UNCITRAL texts, such as article 38 of the CISG, and is intended to allow the mode of provision and other relevant factors to be taken into account.

[28] *Conformity of the data – general*: Article 8 reproduces article 7 of the second revision, which in turn was based on rules set out in the initial draft, revised to reflect suggestions made at the sixty-fifth session (A/CN.9/1132, paras. 33–37), sixty-sixth session (A/CN.9/1162, paras. 81–83) and sixty-seventh session (A/CN.9/1197, paras. 52–60).

[29] *Conformity of the data – interaction between paragraphs 1, 2 and 3*: The chapeau of paragraph 2 has been revised, in response to an exchange at the sixty-seventh session, to clarify that the standards listed in that paragraph (which may be excluded under article 3) supplement the standard in paragraph 1 (A/CN.9/1197, para. 60). In doing so, it does not take a position on whether such standards are characterized as "implied" terms or warranties. To reinforce the point that both paragraphs 1 and 2 address conformity standards, the words "under paragraphs 1 and 2" have been inserted into the chapeau of paragraph 5. The requirements for data to be provided lawfully and free from any third party right or claim have been grouped in an additional paragraph (paragraph 3) in recognition that these standards are not 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 under article 3 or article 8(4).

[30] *Conformity of the data – fitness for ordinary purposes*: The standard in subparagraph 2(a) was included in the initial draft. It was not retained in the first revision following deliberations at the sixty-fifth session, where it was suggested that the standard was excessively prescriptive and that it was preferable to refer to a more flexible notion covering a broad range of data uses (A/CN.9/1132, para. 36). It was also noted that determining the purpose of the use of data could pose challenges. The standard was reinserted following the deliberations at the sixty-sixth session (A/CN.9/1162, para. 82). At that session, the need for data to be "usable" was also emphasized (A/CN.9/1162, para. 77), which was a theme that carried over to the sixty-seventh session. At the latter session, the challenge of determining the purposes for which the data could be used was reiterated, and it was observed that the usefulness of data could vary depending on the industry and role played by the data recipient (A/CN.9/1197, para. 53). It was also pointed out (albeit in the context of the passive provision of data) that the data provider may have little control over what data is provider, particularly in the case of a data generated by a connected device. These observations suggest that, rather than being removed, the standard in subparagraph 2(a) should be adapted to the nature of data transactions, in keeping with the observations in paragraph 7 of the cover note. An alternative formulation of the standard along these lines has

(b) Be 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;

(c) Possess the characteristics which the data provider has held out to the data recipient as a sample or model; and

(d) Possess the characteristics in accordance with any representations that the data provider makes with respect to the data.

3. The data shall be provided:

(a) In compliance with applicable law;[31] and

(b) Free from any right or claim of a third party which impedes the use of the data under the contract or these rules and of which, at the time of the conclusion of the contract, the data provider knew or could not have been unaware.[32]

4. Where appropriate, the parties shall agree on procedures for assessing the conformity of the data and remedying any lack of conformity.[33]

5. In assessing whether the data conforms with the contract under paragraphs 1 and 2, 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 under paragraph 4 or applicable industry standards.

[6. The data recipient shall notify the data provider of any lack of conformity of the data within a reasonable time after discovering it.][34]

---

been included for the consideration of the Working Group. A similar standard is established in the ALI/ELI Principles for "contracts for the transfer of data" and "contracts for simple access to data", namely that the data be "of a quality that may reasonably be expected in a transaction of the relevant kind", provided that "the supplier is in the business of supplying data of the sort that is the subject of the contract or otherwise holds itself out as having expertise with respect to data of that sort". The Working Group may wish to consider whether this alternative formulation is more appropriate to the various types of data provision contracts covered.

[31] *Conformity of the data – lawfulness of provision*: A requirement for the data to be "provided lawfully" was previously included among the supplementary conformity standards. At the sixty-sixth session of the Working Group, support was expressed for recasting the requirement as a stand-alone provision (A/CN.9/1162, para. 82). The second revision suggested that it might be sufficient to incorporate the requirement as a factor to consider in assessing conformity. Following the deliberations at the sixty-seventh session (A/CN.9/1197, para. 57), the requirement has been recast as a supplementary conformity standard. The standard has been included in a separate paragraph for the reasons given in note 29 above.

[32] *Conformity of the data – freedom from third-party rights and claims*: This standard substitutes article 11(2)(c) of the second revision. It has been relocated and reformulated following a suggestion made at the sixty-seventh session (A/CN.9/1197, para. 71). It has been included in a separate paragraph for the reasons given in note 29 above. For an overview of how the rule has evolved, see remarks in the second revision (A/CN.9/WG.IV/WP.186, paras. 61–64). The concept of "right or claim" is intended to cover the concept of "data rights" (see A/CN.9/1117, paras. 27–28), which covers a broader range of rights and claims than those envisaged in article 42 of the CISG.

[33] *Conformity of the data – agreements on data conformity matters*: Paragraph 4 reproduces article 11(2)(b) of the second revision. It has been relocated following deliberations at the sixty-seventh session (A/CN.9/1197, para. 71). The rule was inserted in the first revision in response to observations at the sixty-fifth session about assessing data conformity in practice (A/CN.9/1132, para. 37). In the second revision, the rule was incorporated into a new rule on cooperation between the parties following deliberations at the sixty-sixth session (A/CN.9/1162, para. 80).

[34] *Conformity of the data – notification of lack of conformity*: Paragraph 6 reproduces article 10(2) of the second revision. It has been relocated following a suggestion made at the sixty-seventh session (A/CN.9/1197, para. 70). It has been placed in square brackets following another

[7. As between the parties, the data provider shall not bear the legal consequences of any lack of conformity of the data under paragraphs 2 or 3 if, at the time of the conclusion of the contract, the data recipient knew or could not have been unaware of such lack of conformity.][35]

Article 9. Use of the data[36]

1. Subject to paragraph 2, as between the parties to the contract:[37]

(a) The data recipient is entitled to use the data [in perpetuity][38] for any lawful purpose and by any lawful means[, except that the data recipient is entitled to provide the data to a third party only as agreed by the parties[39]];

(b) The data provider is entitled to continue using the data [only as agreed by the parties].[40]

2. If the data is provided under paragraph (b) of article 6:

(a) The data provider shall provide the data recipient with the means necessary to use the data under the contract and these rules;[41]

---

suggestion that the rule is unnecessary in an online environment (ibid.). The Working Group may wish to confirm whether the rule can be deleted, in which case any duty to notify would be a matter for agreement of the parties under paragraph 4. Paragraph 6 is the only element that remains of the rules on detecting and notifying lack of conformity that were included in the initial draft on the basis of articles 38 to 39 of the CISG. During the sixty-fifth session, doubts were raised as to the applicability of those rules to data transactions (A/CN.9/1132, para. 37). Paragraph 6 also sits uncomfortably with the obligation in article 11(3).

[35] *Conformity of the data – legal consequences of lack of conformity*: Paragraph 7 is new and has been included for the consideration of the Working Group in view of questions raised at the sixty-seventh session regarding the legal consequences of non-performance (A/CN.9/1197, paras. 68 and 71). The rule is based on articles 35(3) and 42(2)(a) of the CISG.

[36] *Use of the data – general*: Article 9 reproduces article 8 of the second revision, which in turn was based on the rules set out in the initial draft. It has been revised to reflect the suggestions made at the sixty-fifth session (A/CN.9/1132, paras. 38–46), sixty-sixth session (A/CN.9/1162, paras. 84–85) and sixty-seventh session (A/CN.9/1197, paras. 61–63).

[37] *Use of the data – mutuality of obligations*: The first revision imposed additional obligations on the data recipient with a view to promoting a mutuality of obligations between the data provider and data recipient (A/CN.9/1132, paras. 41–45), including an obligation to ensure that the data is not used in a manner that infringes the rights of the data provider or of a third party. This obligation was not retained in the second revision to reflect a suggestion at the sixty-sixth session (A/CN.9/1162, para. 85). In view of the limitations on the rights of the data recipient introduced in article 9 (see note 39 below), and concerns to avoid circumventing the basic regime regarding the use of data (see note 45 below), the Working Group may wish to consider reintegrating such an obligation, possibly in conjunction with an obligation on the data recipient to comply with any limitations as to purpose and means of use that are specified in the contract.

[38] *Use of the data – period of time*: The words “in perpetuity” have been inserted to reflect a suggestion at the sixty-seventh session to include a default rule entitling the data recipient to use data, other than data provided under article 6(b), in perpetuity (see A/CN.9/1197, para. 63).

[39] *Use of the data – onward disclosure of the data by the data recipient*: The text in square brackets in subparagraph 1(a) has been included for the consideration of the Working Group. It reflects a suggestion at the sixty-seventh session (A/CN.9/1197, para. 62). It was reasoned that such a rule would guard against circumventing any default rule that limited the period of time for which the data recipient was entitled to use the data and might help to forestall abusive market practices (ibid.).

[40] *Use of the data – continued use of the data by the data provider*: The text in square brackets in subparagraph 1(b) and subparagraph 2(c) has been included for the consideration of the Working Group. It reflects a suggestion at the sixty-seventh session (A/CN.9/1197, para. 62).

[41] *Use of the data – providing means to use the data*: Subparagraph 2(a) was inserted in the second revision. It is intended to balance the right of the data recipient to use the data against the control of the data provider over the information system in which the data is used (see A/CN.9/WG.IV/WP.186, paras. 43–44). It is concerned with technical means, such as software and applications to use the data, which effectively determine the scope of operations (including exporting data from the system) that can be performed on the data and the period of time in which they can be performed (A/CN.9/1197, para. 63). The reference to “appropriate means” has been replaced with “the means necessary” to reflect a suggestion made at the sixty-seventh

(b) The data recipient shall apply those means and is entitled to use the data within the limits of those means;[42]

(c) [The data provider is entitled to continue using the data, including by providing it to a third party.][43]

Article 10. Derived data[44]

1. As between the parties to the contract, the data recipient is entitled to use any data that it generates ("derived data") by processing the data provided under the contract, including by combining the data with other data[, except that the data recipient is entitled to provide derived data to a third party only if it is sufficiently distinct from the data provided under the contract].

[2. In determining whether the derived data is sufficiently distinct for the purposes of paragraph 1, regard is to be had to:

(a) Whether data that is essentially identical to the data provided under the contract can be generated by processing the derived data, including by way of reverse engineering; and

(b) Whether the derived data can be used as a substitute for the data provided under the contract.][45]

Article 11. Common obligations of the data provider and data recipient[46]

1. Each party shall cooperate with the other party when such cooperation may reasonably be expected for the performance of that party's obligations under the contract and these rules.[47]

---

session (ibid.). The words "under the contract and these rules" have been inserted for added clarity.

[42] *Use of the data – applying the means to use the data*: Subparagraph 2(b) brings together the rule obliging the data recipient to apply the means provided by the data provider to use the data (previously in subparagraph 2(a)) and the rule limiting the time period in which the data recipient is entitled to use the data (previously in subparagraph 2(b)). At the sixty-sixth session, it was suggested that the latter rule should be amended to refer to contract expiration, or alternatively to defer to the rules of the system. The Working Group may wish to consider whether it is sufficient to state generally that the data recipient is "entitled to use the data within the limits of those means" on the understanding that such means may control not only the scope of operations that that can be performed on the data, but also the period of time in which they can be performed (see note 41 above).

[43] *Use of the data – continued use of the data by the data provider*: See note 40 above.

[44] *Derived data – general*: Article 10 reproduces article 9 of the second revision, which in turn was based on the text of a proposal put forward at the sixty-fifth session (A/CN.9/1132, paras. 48–49). Apart from the revisions explained in note 45 below, it has been revised to reflect suggestions made at the sixty-sixth session (A/CN.9/1162, para. 86) and sixty-seventh session (A/CN.9/1197, paras. 64–67).

[45] *Derived data – distinctness*: Article 10 has also been substantially revised to address a concern, repeated within the Working Group, that "derived data" should be sufficiently distinguished from the data provided under the contract to avoid rights in derived data under article 10 circumventing any limitations on the rights of the data recipient under article 9 (A/CN.9/1162, para. 86; A/CN.9/1197, para. 65). The revisions, comprising the insertion of text in paragraph 1 and the insertion of paragraph 2, are based on a summary review of standard form contracts used in various industries, primarily for the provision of market data. The revisions are placed in square brackets for the consideration of the Working Group.

[46] *Common obligations – general*: Article 11 was inserted in the second revision. It consolidated various rules on cooperation contained in the first revision which have been revised to reflect suggestions made at the sixty-sixth session (A/CN.9/1162, paras. 80) and sixty-seventh session (A/CN.9/1197, para. 71).

[47] *Common obligations – general duty to cooperate*: Paragraph 1 responds to a suggestion at the sixty-sixth session to replace specific rules in the first revision on cooperation of the parties with a general provision on the conduct of the parties (A/CN.9/1162, paras. 80; see also A/CN.9/1132, para. 43). It has been revised to reflect a suggestion made at the sixty-seventh session to align the rule more closely to article 5.1.3 of the 2016 UNIDROIT Principles of International Commercial Contracts (A/CN.9/1197, para. 71).

2. Each party shall give notice to the other party of any data breach affecting the provision of the data within a reasonable time after becoming aware of the data breach.[48]

3. Each party shall give notice to the other party of any impediment to the use of the data arising from a right or claim of a third party without delay after becoming aware of the right or claim.[49]

Article 12. Non-performance[50]

1. Nothing in these rules affects the application of any rule of law that may govern the legal consequences of a failure of a party to perform its obligations under the contract or these rules.[51]

[2. If the data provider fails to perform its obligations under articles 6 or 7, the data recipient may require performance by the data provider in accordance with applicable law.]

[3. 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 recipient erasing the data from any information system under its control, provided that the data provider remains in a position to use the data.]

---

[48] *Common obligations – duty to notify data breaches*: Paragraph 2 reproduces subparagraph 2(a) of the second revision, which in turn reproduced article 5(3) of the first revision. The scope of the rule is discussed in the second revision (see A/CN.9/WG.IV/WP.186, para. 56). It has been reformulated as a stand-alone rule in response to a suggestion made at the sixty-seventh session (A/CN.9/1197, para. 71).

[49] *Common obligations – duty to notify impediments*: Paragraph 3 reproduces subparagraph 2(d) of the second revision, which in turn was based on article 8(3)(b) of the first revision. It has been revised to reflect the deliberations at the sixty-sixth session (A/CN.9/1162, para. 85) and sixty-seventh session (A/CN.9/1197, para. 71). The wording has also been revised to align with article 8(3)(b).

[50] *Non-performance – general*: Article 12 reproduces article 10 of the second revision and has been revised to reflect deliberations at the sixty-seventh session (A/CN.9/1162, paras. 68–70). Paragraphs 2 and 3 reproduce articles 10(1) and 10(3), respectively, of the second revision. They have not been revised, but rather placed in square brackets pending consideration by the Working Group of the remarks in paragraphs 18–20 of the cover note.

[51] *Non-performance – preservation of remedies under applicable law*: Paragraph 1 reproduces article 10(4) of the second revision. It has been relocated following a suggestion made at the sixty-seventh session (A/CN.9/1197, para. 68).