United Nations A/CN.9/WG.IV/WP.180

General Assembly

Distr.: Limited
14 February 2023

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixty-fifth session
New York, 10–14 April 2023

Default rules for data provision contracts

Note by the Secretariat

Contents

V.23-02664 (E)

I. About this note

1. This note deals with the topic of data provision contracts, which is the focus of the work of Working Group IV on data contracts. Background information on the topic – including the preliminary discussion within the Working Group at its sixty-third session (New York, 4–8 April 2022) and the consideration of the topic within the Commission at its fifty-fifth session in 2022 – is set out in the provisional agenda (A/CN.9/WG.IV/WP.178, paras. 5–7).

2. After proposing a glossary of terms (section II), this note puts forward draft text as a basis for possible default rules for data provision contracts, which builds on preparatory work carried by the secretariat (section III). It also provides the Working Group with an update on relevant national and transnational data-related initiatives that intersect with work on data provision contracts (section IV). At its sixty-fifth session, the Working Group may wish to consider the draft text, and task the secretariat with developing the default rules further, with accompanying commentary, for consideration at the sixty-sixth session, which is tentatively scheduled for 16–20 October 2023.

II. Glossary of terms

3. The Working Group may wish to consider the terms defined in this section as a basis for establishing a common understanding of the subject matter, as well as for defining the substantive scope of its work.

A. "Data"

4. Based on the widely-used definition formulated by the International Organization for Standardization, and using the language of existing UNCITRAL texts on electronic commerce, the secretariat has developed the following working definition of "data", which was presented to the Working Group at its sixty-third session (A/CN.9/1093, para. 85):

"Data" is as a representation of information in electronic form.

5. This working definition of "data" covers a wide variety of information that has become the subject of commercial transactions, including market analysis data and operational data (e.g., data generated by sensors attached to machines). Data within the definition can be categorized into different types. It can be characterized as "raw" (unprocessed) or "derived" (produced by processing other data). It can also be categorized by reference to (i) the person who controls the data (e.g. public data, private data), (ii) the person to whom the data relates (e.g. personal data[1]), (iii) the content of the data (e.g. proprietary data,[2] corporate data, technical data), (iv) the purpose for generating the data,[3] or (v) the format of the data (e.g. structured data, unstructured data). On the inclusion of "personal data" within scope, see discussion below (paras. 8–9).

6. By focusing on data as a representation of "information", the working definition allows certain types of data to be distinguished, including software (i.e. data comprising computer code) and digital assets (i.e. data comprising an electronic

[1] The term "personal data" is widely used to refer to data relating to an identified or identifiable natural person.

[2] The concept of "proprietary data" is understood as data that is subject to "data rights", in particular the protections afforded under laws relating to trade secrets, copyright and database rights.

[3] The purpose for generating the data is used by the World Bank to distinguish "public intent data" and "private intent data": *World Development Report 2021: Data for Better Lives* (Washington, 2021).

record that is capable of being controlled and uniquely identified). Transactions in software and digital assets are not concerned with data as a representation of "information" – in the sense of material that can be given meaning in a particular context – but rather with data as the means to effect processes that give software and digital assets their value. At the sixty-third session of the Working Group, it was suggested that relying on data as a representation of "information" could be considered as a starting point for distinguishing – and possibly excluding from scope – dealing in digital assets (A/CN.9/1093, para. 85). The Working Group may wish to consider further how to deal with contracts for the supply of software and digital assets.

7. By focusing on data "in electronic form", the working definition recognizes the quality of machine-readability – and thus suitability for automated processing – that gives data its value in the digital economy. It also emphasizes the peculiar qualities of data as intangible and non-rivalrous (in the sense that the use of data by one person does not limit its use by another person).

8. The Commission has previously indicated that future work on data transactions should avoid data privacy and protection issues, as well as intellectual property issues. At its sixty-third session, the Working Group engaged in a discussion about what it means for future work to "avoid" data privacy and protection issues, given the many jurisdictions have data privacy and protection laws in place to regulate the processing of personal data. In summary, the following views were exchanged:

(a) Avoiding data privacy and protection issues means that future work should not only be aware of relevant laws, but also refrain from harmonizing regulatory measures concerning the processing of personal data. It also means that a baseline for future work should be a requirement that data be acquired, provided and otherwise processed "lawfully" (akin to the treatment of prohibited goods in sale of goods contracts);

(b) Avoiding data privacy and protection issues does not mean that future work should ignore data that, in a particular jurisdiction, is regarded as "personal data". It would be impractical – if not impossible – to limit the scope of future work to data other than personal data.

9. The Working Group may wish to confirm that approach, which is consistent with the various national and transnational data-related initiatives mentioned in section IV of this note. It may thus wish to confirm that its work should proceed on the basis that:

(a) Default rules should not exclude personal data from scope;

(b) Default rules should preserve regulatory measures under existing data privacy and protection laws (see, e.g., article 2(4) of the 2022 UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT)).

10. It may also wish to consider addressing the impact of the lawfulness of acquisition, provision and use from the perspective of both warranties on the part of the data provider (see paras. 34 and 40 below) and remedies, such as avoidance of the contract for breach of those warranties (see para. 46 below).

B. "Processing"

11. The concept of "processing" data is key to understanding the rights and obligations of the parties to data contracts. Based on existing domestic and international sources, the secretariat has developed the following working definition of "processing", which was presented to the Working Group at its sixty-third session (A/CN.9/1093, para. 86):

"Processing" data is any one or more operations performed on data.

12. Domestic and international sources often list examples of operations performed on data, including collecting, recording, organizing, structuring, altering, storing, retrieving, transmitting and erasing data. Some sources refer to "generating" data. Some refer to data being "accessed" or "shared",[4] or to a person "using" or "disclosing" the data,[5] which may involve the performance of several operations. Some also refer to a person "controlling" data, and to data being "transferred" or "ported"[6] to effect a change in control. As elaborated below (para. 42), the Working Group may wish to exercise caution in using terminology around the "control" of data, which may be laden with legal connotations. It may wish to consider whether it is sufficient to refer generally to the "processing" of data, which may also provide for a more technology-neutral and future-proof text.

C. "Data provision contract"

13. The secretariat has developed the following working definition of "data provision contract", which was presented to the Working Group at its sixty-third session (A/CN.91093, para. 89):

> *A "data provision contract" is a contract for the provision of data, under which one party (the "data provider") provides (or supplies) data to another party (the "data recipient").*

14. Many contracts involve the exchange of data or data messages but are not contracts for the provision of data (i.e. the subject of the contract is not the data). For instance, a contract is not a "data provision contract" merely because it is concluded in electronic form, or because it involves a party (or a device controlled by the party) sharing information in electronic form. Moreover, in the context of consumer contracts (addressed further in para. 16 below), a contract for the supply of services is not a "data provision contract" merely because the consumer provides personal data as "consideration" for receiving the service.

15. There are various modes by which data can be provided. The data provider may provide the data by "sharing" the data with the data recipient or by giving the data recipient "access" to the data or to a data source. Data provision contracts are thus sometimes referred to as "data sharing contracts" or "data access contracts". In both cases, the terminology suggests that the data provider retains a residual entitlement to use the data. The term "data sharing" also suggests that both parties are providing data to one another, which also occurs under "data pooling" arrangements, where the parties contribute data to a "data pool". The Working Group may wish to consider whether such arrangements should fall within the scope of future work, noting that data pooling arrangements may exhibit traits of "data processing contracts", which are discussed below (paras. 17–20).

16. While not strictly a definitional issue, the Working Group may wish to consider the necessity or desirability of excluding from scope data provision contracts with consumers, in line with the approach taken in the United Nations Convention on Contracts for the International Sale of Goods (CISG) and the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC). While data provision contracts with consumers may not be common (as opposed to data processing contracts or contracts for the supply of data products such

[4] The OECD recommendation on enhancing access to and sharing of data (see footnote 15 below) defines "data access" as the act of "querying or retrieving data for its potential use" and "data sharing" as the act of "providing data access for use by others".

[5] See, e.g., EU, Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union.

[6] At the sixty-third session of the Working Group, it was explained that data "porting" 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).

as digital assets or services provided by electronic means), the Working Group may nevertheless wish to consider the interaction between default rules and data related to consumer behaviour, which may be subject to specific regulation. Other exclusions from the scope of default rules could be considered (including contracts for the supply of software and digital assets, discussed in para. 6 above).

D. "Data processing contract"

17. At the sixty-third session of the Working Group, broad support was expressed for distinguishing data provision contracts and data processing contracts (A/CN.9/1093, para. 89). The following working definition of "data processing contract" was presented to the Working Group (ibid.):

> *A "data processing contract" is a contract under which one party (the "service provider") processes data for another party (the "service recipient") and provides the processed data to the other party.*

18. This definition covers a range of data transactions, including data scraping, cloud-based services, data analytics, and electronic transmission services.

19. The Commission took note of the distinction at its fifty-fifth session (A/77/17, para. 161). Support was expressed to continue work on data processing contracts, although it was suggested that, for the time being, such work should be limited to monitoring legislative developments. Accordingly, the Commission requested the secretariat to continue monitoring legislative developments (A/77/17, para. 163).

20. Admittedly, the distinction between data provision contracts and data processing contracts is not always clear-cut, akin to the distinction between contracts for the sale of goods and contracts for the delivery of labour and services under article 3 of the CISG. An example given at the sixty-third session of the Working Group was data sharing arrangements using third-party platforms, such as a "data marketplaces", which play a significant role in the data "ecosystem". Third-party platforms may also be used to support "data pools" (see para. 14 above). While these arrangements are ultimately designed for data sharing, the individual contracts involved tend to be data processing contracts between the platform provider and the platform user, albeit on terms that contemplate the processed data being provided to other platform users. Nevertheless, data sharing platforms can be used for data transactions between platform users and, in some jurisdictions, have been the focal point for initiatives aimed at promoting legal certainty regarding data contracts (see, e.g., the initiatives in China mentioned in para. 50 below). Moreover, the significance of data sharing platforms for data sharing arrangements has meant that they have been addressed alongside data provision contracts in other initiatives (see, e.g., the initiatives in Japan and the Republic of Korea mentioned in paras. 49 and 50 below, respectively).

E. "Data ecosystem"

21. At the sixty-third session of the Working Group, it was stressed that future work on data contracts should take into account the complexities of the "data ecosystem". Data is transacted along a "data value chain" which involves multiple actors performing a range of (often overlapping) roles with respect to data to generate value. This includes: (i) persons who generate data (including "raw" data generated by machines or sensors), (ii) persons to whom data relates, whether a legal person or natural person (i.e., the "data subject"), and (iii) persons who process the data to generate "derived" data (e.g., by performing any of the operations listed in para. 12 above, whether for themselves or as a service provided to others, not to be confused with the concept of "data processor", which is a term of art in some data privacy and

protection regimes). The various actors and operations performed on data, together with the data transactions between them, comprise the "data ecosystem".[7]

III. Draft default rules for data provision contracts

A. Introduction

22. At its fifty-fifth session, the Commission heard views, but took no decision, on the form and legal nature of the output of the Working Group on data provision contracts. It was recalled that several options had been canvassed at the sixty-third session of 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 (A/77/17, para. 164). Default rules need not be contained only in a legislative text; for instance, at the sixty-third session, it was acknowledged that default rules could take the form of "hard law" (e.g. conventional or legislative rules) and "soft law" (e.g. contract or legislative guides). At the same time, the importance of the principle of party autonomy was stressed, regardless of the form of the eventual output (A/CN.9/1093, para. 95). The default rules set out in this section have been formulated in a manner that is neutral as to form.

23. At the sixty-third session of the Working Group, it was recalled that the secretariat had been examining the provisions of the CISG as a possible source of inspiration for establishing default rules for data provision contracts (A/CN.9/1093, para. 90). The secretariat has adopted a cautious approach in doing so, not wishing to open discussions on whether a data provision contracts can be characterized as a "contract for sale" or whether data can be characterized as "goods".[8] For that reason, it has suggested that, rather than adapt specific provisions of the CISG to data provision contracts, the legal issues dealt with in the CISG – particularly the rights and obligations of the parties and remedies for breach of contract – could be seen as a reference point for future work on data provision contracts. The Working Group may wish to consider whether such a methodology is appropriate for its work on data provision contracts.

24. Leaving aside questions of characterization, further work to develop default rules should take account of the differences in the commercial relationships and transactions involved in sale of goods and data provision arrangements.[9] For instance:

(a) Data provision contracts tend to be more relational than sale of goods contracts, in the sense that they involve the provision of data as part of an ongoing relationship (although the CISG does make special provision for instalment contracts);[10]

(b) The intangible nature of data and its suitability for automated processing mean that real-time or continuous supply is particularly important for data provision contracts;

(c) The non-rivalrous nature 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;

---

[7] The OECD recommendation on enhancing access to and sharing of data (see footnote 15 below) defines the "data ecosystem" as "the integration of and interaction between different relevant stakeholders including data holders, data producers, data intermediaries and data subjects, that are involved in, or affected by, related data access and sharing arrangements, according to their different roles, responsibilities and rights, technologies, and business models".

[8] For a recap of those discussions, see A/CN.9/1012/Add.2, paras. 42–45.

[9] The differences between data flows and cross-border trade in goods and services is highlighted by UNCTAD in the most recent Digital Economy Report; *Digital Economy Report 2021 – Cross-border Data Flows and Development: For Whom the Data Flow* (Geneva, 2021), pp. 74–76.

[10] The 2016 UNIDROIT Principles of International Commercial Contract contain rules dealing specifically with long-term contracts.

(d) As elaborated below (para. 41), the ability to determine the purposes and means of processing data often depends on contractual rights, while the use of goods depends on rights defined elsewhere (i.e. in property law);

(e) Data provision arrangements are not limited to the provision of data in return for payment, as it the case for the sale of goods. As noted above (para. 15), data provision contracts may involve the provision of data by one party in return for the provision of data by another party, somewhat akin to barter transactions.[11]

25. Bearing this in mind, the secretariat has prepared draft text for possible default rules on the following issues, which build on the proposal to the Commission:

(a) mode of provision (i.e. how the data is provided);

(b) conformity of data (e.g. quality, quantity and fitness for purpose);

(c) rights to process the data (e.g. how the data is used).

26. This draft text and accompanying remarks is presented to the Working Group for consideration. The secretariat has also included remarks on possible default rules on remedies for breach. Other default rules not covered in this note can be envisioned, such as rules on payment.

B. Rules on mode of provision

27. Under the CISG, delivery of the goods constitutes the seller's primary obligation under a sales contract. Article 31 establishes rules on the place of delivery, and provides for the seller to hand the goods over to a third party carrier for transmission to the buyer or to place them at the disposal of the buyer. Those rules could be transposed and adapted to data provision contracts. In the proposal, the secretariat noted that such rules could accommodate the different modes by which data is provided in practice, and a proviso that the mode of providing the data be reasonable in the light of data security concerns. Rules to that effect can be inspired by the recent work of the Working Group on identity management and trust services, and use the language of UNCITRAL texts on electronic commerce (e.g., transmission of data between "information systems").

28. The Working Group may wish to discuss possible rules on the mode of providing the data on the basis of the following text:

(1) Except where the parties have agreed otherwise, the data provider provides the data to the data recipient by transmitting it to an information system designated by the data recipient.

(2) If the data provider provides the data to the data recipient by giving the data recipient access to the data in a system under the control of the data provider that enables the data recipient to process the data under the contract:

(a) the data provider provides means for the data recipient to access the data; and

(b) the data recipient complies with the reasonable data security requirements of the data provider.

29. Article 33 of the CISG establishes rules on the timing (including periodicity) of delivery. It defers to the delivery date or period that is fixed or determinable in the contract and, as a default rule, provides for the seller to deliver the goods "within a reasonable time after the conclusion of the contract". Those rules could be transposed and adapted to data provision contracts.

[11] Barter transactions and other "countertrade transactions" in the 1992 UNCITRAL Legal Guide on International Countertrade Transactions.

30. The Working Group may wish to discuss rules on the timing of providing the data on the basis of the following text:

The data provider provides the data according to the timeframe fixed or determinable from the contract or otherwise within a reasonable time.

31. A default rule for data to be provided "within a reasonable time" may be useful where the data is continuously generated by a sensor or other data source under the control of the data provider. In some circumstances, it might be reasonable for that data to be provided in real-time. However, the reference to provision "within" a certain "time" may need to be revisited to better accommodate continuous data feeds.

32. An additional issue associated with the mode of provision is the risk of data loss or alteration during transmission. The Working Group may wish to consider how the use of electronic transmission services (e.g. "electronic registered delivery services" within the meaning of the MLIT) could be incorporated into data provision contracts to address that risk. The issue of data loss or alteration during transmission is also a matter of the conformity of data, which is addressed below (see para. 38).

C. Rules on the conformity of data

33. Article 35 of the CISG establishes rules on the conformity of goods. The primary test for conformity in article 35(1) defers to the terms of the contract as to the "quantity, quality and description" of the goods, and to the manner in which the goods are contained or packaged. Article 35(2) then establishes a default rule, which requires the goods to be fit for ordinary purposes or for particular purposes made known to the seller, to possess the qualities held out via any sample or model, and to be packaged in the usual or an adequate manner.

34. The elements of conformity in the CISG – quantity, quality, fitness for purpose and reference to samples and models – can readily be transposed and adapted to data and are important elements of data provision contracts. For instance, the quantity of data would encompass the frequency in which the data is provided, while the quality of data would encompass data-specific characteristics such as accuracy and currency. The quality of data would also encompass "traceability", which incorporates assurances as to the origin and integrity of data, and "lawfulness", which incorporates assurances that the data being provided complies with legal requirements (which is linked to warranties as to the use of the data by the data recipient, discussed in para. 41 below). The description of the data would encompass format, as well as characteristics to delimit the scope of data, such as the level of granularity (i.e. the precision of the data) and the types of data that are to be included or excluded (e.g., the types listed in para. 5 above). It is worth noting that, even if "personal data" is included within scope (see para. 9 above), the parties may well agree to expressly exclude that type of data from the scope of the contract, particularly in view of restrictions on the transfer of personal data under applicable data privacy laws.

35. Moreover, a fitness for purpose test can be applied to data, and the use of sample data is not uncommon in the data marketplace. A question remains, however, whether the standards reflected in the default rule of the CISG set the right balance for data provision contracts. In that regard, the view was expressed at the sixty-third session of the Working Group that the contract price was an important consideration in assessing the conformity of the data (A/CN.9/1093, para. 90).

36. The Working Group may wish to discuss rules on the conformity of data on the basis of the following text:

(1) The data provider provides data which is of the quantity, quality and description required by the contract.

(2) Except where the parties have agreed otherwise, the data conforms with the contract if:

(a) it is fit for the purposes for which data of the same description would ordinarily be used;

(b) 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;

(c) it possesses the qualities of data which the data provider has held out to the data recipient as a sample or model.

37. Articles 38 to 40 of the CISG require the buyer to inspect the goods and give notice of any lack of conformity. These rules could also be tailored to data provision contracts. The relevance of determining conformity in the context of data provision contracts is underscored in the proposal for a "Data Act" in the European Union (EU), which treats as "unfair" and unenforceable terms in data contracts with micro, small and medium-sized enterprises that give the other party the exclusive right to determine whether data provided is in conformity with the contract. The Working Group may wish to discuss rules on detecting and notifying lack of conformity on the basis of the following text:

(1) The data recipient examines the data, or causes it to be examined, within as short a period as is practicable in the circumstances.

(2) The data recipient loses the right to rely on a lack of conformity of the data if it does not give notice to the data provider specifying the nature of the lack of conformity within a reasonable time after the data recipient detected it or ought to have detected it.

(3) The data provider is not entitled to rely on paragraph (2) if the lack of conformity of the data relates to facts of which the data provider knows or could not be unaware and which the data provider does not disclose to the data recipient.

38. Article 35 of the CISG deals with the time at which the lack of conformity is to have arisen, which is linked to the passing of the risk in the goods, which in turn is linked to remedies. The Working Group may wish to consider whether it is sufficient for lack of conformity to have arisen at the time the data was provided to the data recipient (according to the rules on mode of provision above). A related issue that the Working Group may wish to consider is whether the data recipient should bear the risk of data loss or alteration during transmission.

D. Rules on the use (or processing) of data

39. At the sixty-third session, the view was expressed that, from the perspective of the data recipient, it was important to include an assurance that the data was lawfully provided and could lawfully be processed (A/CN.9/1093, para. 90). Articles 41 and 42 of the CISG require the seller to deliver goods that are free from any right or claim of a third party, including rights based on industrial property or other intellectual property. Rights and claims based on industrial property or other intellectual property, in particular copyright and trade secrets, can also affect use of data, as can rights and claims under data privacy and protection laws (e.g., in the case of data that is personal data) and laws relating to database rights.

40. Ordinarily, the data recipient should be put in a position by the data provider to use the data and any derived data for the purposes of the contract free of any such rights and claims of any third party (i.e. other "data rights", as described in paras. 26–27 of A/CN.9/1117). Already at the sixty-third session of the Working Group, it was

foreshadowed that future work could focus on assurances that the data was lawfully acquired and provided and could lawfully be processed under the contract. In that regard, it was suggested in particular that data provision contracts should warrant that the data provided by the data provider and that the intended use of the data by the data recipient complies with applicable laws relating to data privacy.

41. However, it may not be enough for data provision contracts to regulate the use of data in such negative terms. Owing to the nature of "goods" as an object of property rights, as well as the characteristics of "sales" 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. For its part, owing to its peculiar qualities (see para. 7 above), data is generally not recognized as an object of property rights (see A/CN.9/1117, para. 47).[12] It is therefore not amenable to ownership nor to the rights that the law attributes to ownership. Given the "patchwork" of data rights under other legal regimes described in the proposal (A/CN.9/1117, para. 46), data contracts remain a primary source of law governing the use of data. For that reason, it is important for data provision contracts to regulate the use of data in positive terms. Moreover, given the non-rivalrous nature of data, this covers not only use by the data recipient but also residual use by the data provider.

42. At this point, it is convenient to recall that the Commission has not referred the topic of "data rights" to the Working Group, but has instead requested the secretariat to continue preparatory work on the topic (A/77/17, para. 163). It is also convenient to draw the attention of the Working Group to terminology for formulating rules on the use of data:

(a) *Use* – As noted above (para. 12), the concept of "using" data can involve a range of different operations performed on data. In its ordinary meaning, the concept suggests the processing of data that is within the control of the data processor. Along similar lines, the "use" of data is sometimes used in contrast to the "generation" or "disclosure" of data. To avoid doubt as to the scope of the rights and obligations of the parties, it may be preferable for rules of the use of data to refer to the "processing" of data;

(b) *Control* – The rights acquired in data are sometimes referred to in terms of "control". The concept of "controlling" data is open to different meanings. It was already observed at the sixty-third session of the Working Group that the term "control" would need to be clearly defined (A/CN.9/1093, para. 86). The term "controller" has developed a special meaning in the context of data privacy and protection, where it refers to the person with power (in law or in fact) to determine the purposes and means of processing personal data.[13] The Principles for a Data Economy, jointly developed by the American Law Institute and European Law Institute (hereafter the "ALI/ELI Principles"), apply the term to all types of data and, in the context of data provision, refer to the data provider putting the data recipient in "control" of the data in the sense of removing legal barriers to the data recipient determining the purposes and means of processing the data. In other contexts, the concept of "controlling" data (among other intangibles) is the functional equivalence of possessing tangibles (see, e.g., article 11 of the MLETR), and is used in that sense in paragraph (a) above. To avoid doubt, it may be preferable to refer to the rights of the data recipient to determine the purposes and means of processing data and the obligation of the data supplier to warrant such use free of third-party rights and claims.

43. It is also convenient to recall that rules on the use of data – or rather the processing of data – will depend on whether the contract applies a "sales" approach

[12] The law in some jurisdictions has moved to recognize certain data products (e.g. digital assets) as objects of property rights.

[13] See, e.g., definition of "controller of the file" in article 2(d) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), United Nations, *Treaty Series*, vol. 1496, No. 25702.

or a "licence" approach (see A/CN.9/1093, para. 83). A "sales" approach would suggest a rule that entitles the data recipient to determine the purposes and means of processing the data, as well as a rule that contemplates the data provider giving up any such residual entitlement. Conversely, a "licence" approach would suggest a rule that entitles the data recipient to process the data only as provided for in the contract, which may limit processing by reference to purposes or means, or by reference to particular operations. It might be preferable for the Working Group to avoid the terminology of "sales" and "licences" so as to focus on the content of the rights under the contract.

44. The Working Group may wish to discuss rules on the processing of data on the basis of the following text:

(1) Except where the parties have agreed to limit processing by reference to a specified purpose or means:

(a) the data recipient is entitled to process the data for any lawful purpose and by any lawful means; and

(b) the data provider is entitled to continue processing the data and to provide it to third parties.

(2) If the parties have agreed to limit the purpose for which, or means by which, the data recipient processes the data, the data recipient processes the data in conformity with that purpose or those means.

(3) Subject to paragraphs (4) and (5), the data provider warrants that no right or claim of a third party impedes the processing of the data in accordance with paragraphs (1) or (2). The data provider carries out all formalities required to give effect to this rule.

(4) Paragraph (3) applies only to:

(a) a right or claim of which the data provider knows or could not be unaware at the time of the conclusion of the contract;

(b) a right or claim under the law of the State in which the data is processed, if made known to the data provider at the time of the conclusion of the contract, or otherwise under the law of the State where the data recipient has its place of business.

(5) Paragraph (3) does not apply to a right or claim of which the data recipient knows or could not be unaware at the time of the conclusion of the contract.

45. The Working Group may wish to consider whether specific provision is needed to address rights in derived data (i.e., data produced by either party by processing the data provided under the contract).

E. Rules on remedies for breach

46. The CISG establishes a detailed regime of remedies that are available to either party in the event of breach by the other party. This regime applies to breach of the contract and breach of the default rules established in the CISG. Some of those remedies may not be suitable to data provision contracts, while others may require tailoring (e.g. the duty to make restitution). At its sixty-third session, Working Group IV did not address the issue of remedies. The Working Group may wish to consider whether default rules could be developed to address remedies for breach of data provision contracts or breach of the default rules, taking into account the peculiar qualities of data, and noting potential intersection with ongoing work on the automated performance of contracts (see in particular A/CN.9/1125, para. 35). It is worth noting that the ALI/ELI Principles do not deal with remedies in detail, stating

instead that "remedies with respect to data contracts… should generally be determined by the applicable law".

IV. Intersections with other initiatives

47. During deliberations on the proposal within the Commission, it was emphasized that work on data transactions in general should be mindful of the output of other legislative and non-legislative projects (A/77/17, para. 162).

48. Work on data provision contracts has the potential to complement a range of international initiatives on data governance and cross-border data flows, which are becoming a focus of international trade for all types of data. The link between data provision contracts and international trade was emphasized at the sixty-third session of the Working Group (A/CN.9/1093, para. 92).

(a) One such initiative is an ongoing project among members of the World Trade Organization to negotiate rules that enable and promote the flow of data as part of the Joint Statement Initiative (JSI) on E-Commerce. Drafting proposals published so far focus on overcoming regulatory barriers, such as localization requirements for data processing or other restrictions on the cross-border transfer of data, and on declaring broad policy objectives to establish a permissive regime for data flows that facilitate international trade, such as Data Free Flow with Trust ("DFFT"). The proposals do not address how those data flows are effected or the private law gaps that inhibit them, nor do they mandate harmonized responses to pre-empt fragmented national legislative efforts to fill those gaps, which could create further obstacles to international trade. Future work on data provision contracts could thus provide the basic legal infrastructure to give effect to those policy objectives, much as existing UNCITRAL texts on electronic commerce do for rules enabling e-commerce that are also being negotiated as part of the JSI, and which already exist in bilateral and regional free trade agreements (including dedicated digital trade agreements). So much is recognized in a paper recently published by the World Economic Forum on overcoming barriers to cross-border data flows, which finds that the realization of DFFT requires the development of legal and technological tools to mitigate business risks, including the use of model contractual clauses for cross-border data transfers;[14]

(b) Another such initiative is ongoing work by the Organisation for Economic Co-operation and Development (OECD) to implement the recommendation adopted by the Council of the OECD in 2021 on enhancing access to and sharing of data.[15] The recommendation recognizes that data access and sharing arrangements encompass not only the institutional, regulatory and policy frameworks that determine the conditions of data access and sharing, but also the legal and contractual frameworks. Insofar as the recommendation does not prescribe standards for legal and contractual frameworks (although it does recognize the importance of party autonomy), future work on data provision contracts could provide an important contribution to the development of such standards. It could also contribute to the development of data sharing frameworks to which States are committing themselves under dedicated digital trade agreements;

(c) Yet another such initiative is the proposal by the Secretary-General for a "Global Digital Compact" to advance the commitment of member States to improve "digital cooperation" in the declaration on the commemoration occasion of the seventy-fifth anniversary of the United Nations (A/RES/75/1). Among other things, it is expected that the Global Digital Compact will focus on fostering the safe and responsible use of data. The secretariat suggests that the concepts and rules developed by the Working Group on data provision contracts will provide a useful toolbox for addressing that area.

[14] "Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows" (January 2023).
[15] OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data (2021), document C/MIN(2021)20/FINAL.

49. Work on data provision contracts also has the potential to harmonize a range of national and transnational initiatives that have sought to address legal uncertainty regarding data contracts. Two of these initiatives – the ALI/ELI Principles and the contract guidelines on the utilization of data published by the Ministry of Economy, Trade and Industry of Japan (hereafter the "METI Data Guidelines")[16] – were presented to the Working Group at its sixty-third session (A/CN.9/1093, paras. 80–84). As noted during the presentations, those initiatives take different approaches with respect to data provision contracts. On the one hand, the ALI/ELI Principles set out "default rules" that should be provided by law for inclusion in different types of contracts for the supply or sharing of data. They are designed as both a best practice guide for parties and a legislative and judicial guide. On the other hand, the METI Data Guidelines describe the main issues associated with data contracts and set out "model contract clauses". While both initiatives employ different typologies of data contracts, they both distinguish between contracts that apply a "sales" (or "assignment") approach, and those that apply a "licence" approach as a means to identifying the rights and obligations of the parties.

50. Other initiatives are underway or are contemplated:

(a) In China, several data trading platforms are developing contractual guidelines for parties transacting data via the platform;

(b) In the EU, a proposal by the European Commission for a "Data Act" contemplates the Commission will "develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations";[17]

(c) In India, a proposal for a data accessibility and use policy, with the aim of "enhance[ing] access, quality, and use of data, in line with the current and emerging technology needs of the decade", lists the "absence of innovative licensing frameworks, guidance on licensing approach, pricing datasets, criteria for valuation, and reference valuation models" as one of the "bottlenecks" to improving opportunities in data accessibility and use.[18] The proposal defines "licensing frameworks" as "agreed legal framework for the exchange of data between two or more entities, the permitted use of datasets and the access term for those datasets";

(d) In the Republic of Korea, the Ministry of Trade, Industry and Energy has recently published contract guidelines on industrial data.[19] The guidelines describe the main issues associated with three types of data contracts – data provision, data generation, and data sharing (using a platform) – and provide model contract clauses.

51. The Working Group may wish to take stock of the projects outlined in this section, which may help in shaping its future work. The Working Group may wish to take note of regional initiatives that are aimed at ensuring that contracts for the provision of personal data comply with data privacy and protection laws. Such initiatives include standard clauses promulgated by the European Commission under the General Data Protection Regulation for contracts for data transfers outside the EU, and model clauses for contracts for data transfers between parties in different member States of the Association of Southeast Asian Nations (ASEAN), approved by the ASEAN Digital Ministers in 2021. However, the secretariat considers that these

[16] Japan, Ministry of Economy, Trade and Industry, *Contract Guidelines on Utilization of AI and Data: Data Section* (June 2018), English translation available at www.meti.go.jp/english/press/2019/0404_001.html, p. 1. The METI Data Guidelines (in the original Japanese) have since been updated following the amendments to the Unfair Competition Prevention Act: see www.meti.go.jp/english/press/2019/1209_005.html.

[17] EU, European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and the use of data, document COM(2022) 68 final (23 February 2022).

[18] The draft policy is available at https://meity.gov.in/content/draft-india-data-accessibility-use-policy-2022 (accessed on 8 February 2023).

[19] The guidelines are available at https://idx.or.kr/portal/dx-cooperation-support/contract-guideline/introducion/index.do (accessed on 8 February 2023).

initiatives are of limited relevance to the work of the Working Group insofar as they do not seek to address broader legal issues raised by data provision contracts that are addressed in the draft default rules set out in this note.