United Nations A/CN.9/WG.IV/WP.142

General Assembly

Distr.: Limited
6 February 2017

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-fifth session
New York, 24-28 April 2017

Contractual aspects of cloud computing

Note by the Secretariat

Contents

V.17-00642 (E)

I. Introduction

1. At its forty-seventh session, in 2014, the Commission had before it a proposal by the Government of Canada entitled "Possible future work on electronic commerce — legal issues affecting cloud computing" (A/CN.9/823). The proposal explained the concept of cloud computing and why it would be useful for UNCITRAL to carry out work on the legal issues affecting parties to a cloud computing arrangement. The preparation of "a document outlining the cloud computing contractual relationships and legal issues that arise in that context" was suggested (A/CN.9/823, para. 5). The proposal illustrated a number of such possible legal issues, explicitly excluding intellectual property (IP) and privacy from the scope of the suggested work (A/CN.9/823, paras. 5-11). A checklist or a more detailed list of considerations for cloud users were mentioned as options for a possible form of the document, and a specific reference was made to UNCITRAL documents in other fields, such as the *Notes on Organizing Arbitral Proceedings* (1996),[1] *Recognizing and Preventing Commercial Fraud: Indicators of Commercial Fraud* (2013)[2] and the *Legal Guide on International Countertrade Transactions* (1992)[3] (A/CN.9/823, para. 5). Possible steps by the Commission as regards the proposal were suggested, in particular a request from the Commission to the Secretariat to gather information relating to cloud computing and prepare a document outlining exising practices, which "could then be used by the Working Group to identify issues in need of practical legislative or other solutions and to discuss possible future work" (A/CN.9/823, para. 12).

2. At that session, there was wide support in the Commission for the proposal recognizing the implication of cloud computing, particularly for small and medium-sized enterprises. However, it was suggested that caution should be taken not to engage in issues such as data protection, privacy and IP, which might not easily lend themselves to harmonization and might raise questions as to whether they fell within the mandate of the Commission. It was also stressed that work already undertaken by other international organizations in that area should be taken into consideration so as to avoid any overlap and duplication of work. It was also suggested that compilation of best practices might be premature at the current stage. Subject to those comments, it was generally agreed that the mandate given to the Secretariat should be broad enough to enable it to gather as much information as possible for the Commission to consider cloud computing as a possible topic at a future session. It was noted that the scope of any future work would, in any case, have to be determined by the Commission at a later stage. After discussion, the Commission requested the Secretariat to compile information on cloud computing, including by organizing, co-organizing or participating in colloquia, workshops and other meetings within available resources, and to report at a future session of the Commission.[4]

3. At its forty-eighth session, in 2015, the Commission had before it a proposal by Canada entitled "Contractual issues in the provision of cloud computing services" (A/CN.9/856). The information provided therein was "aimed at advancing the review of legal issues affecting the provision of cloud computing services so that a Working Group can use this preparatory work in developing recommendations" (A/CN.9/856, the last paragraph before the annex). The proposal expanded on the issues identified in document A/CN.9/823 (see para. 1 above), in particular on the concept of cloud computing and its various existing models, characteristics, benefits and risks

[1] Available at www.uncitral.org/uncitral/en/uncitral_texts/arbitration/2016Notes_proceedings.html.
[2] Available at www.uncitral.org/uncitral/en/uncitral_texts/payments.html.
[3] United Nations publication, Sales No. E. 93.V.7 (A/CN.9/SER.B/3), available at www.uncitral.org/uncitral/en/uncitral_texts/sale_goods.html.
[4] *Official Records of the General Assembly, Sixty-ninth Session, Supplement No. 17* (A/69/17), paras. 146, 147 and 150.

(economic, security and legal) (A/CN.9/856, paras. 4-47). A number of legal issues additional to those listed in document A/CN.9/823 were identified (A/CN.9/856, paras. 48-75). An annex to the proposal provided information on international organizations that had covered issues relating to cloud computing in their work. As a possible step by the Commission, it was suggested that the Commission may mandate a Working Group to review legal issues arising from cloud computing and to recommend best practices where needed based on evidence of absence of legal recourses, perceived imbalance between the rights and obligations of cloud computing participants or other evidence. It was further suggested that the Secretariat, in order to assist the Working Group, could conduct research on contractual issues that arise in the provision of cloud computing services and explore possible solutions in relation to some or all of these issues with the view of fostering international trade. Experts meetings and consultations could also be used to gather additional information (A/CN.9/856, the last paragraph before the annex).

4. At that session, broad consensus was expressed in the Commission for undertaking work in the field of cloud computing. It was suggested that that work could take the form of guidance material or as otherwise appropriate, and should cover the perspectives of all parties involved, i.e. service providers, users and concerned third parties. It was further suggested that private international law aspects should be discussed, possibly in cooperation with the Hague Conference on Private International Law. After discussion, the Commission instructed the Secretariat to conduct preparatory work on cloud computing, including through the organization of colloquia and expert group meetings, for future discussion at the Working Group level. The Commission also asked the Secretariat to share the result of that preparatory work with Working Group IV, with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission.[5]

5. At its forty-ninth session, in 2016, the Commission was informed that work on contractual aspects of cloud computing had started at the expert level on the basis of the proposal A/CN.9/856. The Commission was also informed about preparatory work on the other topic allocated by the Commission to the Working Group (identity management and trust services). It was suggested that work should commence on legal issues relating to cloud computing based on preparatory work already conducted. However, the view was also expressed that additional preparatory work was necessary, which should aim at compiling relevant information. Preference was expressed for work to commence instead on identity management and trust services. After discussion, it was generally felt that the topics of identity management and trust services as well as of cloud computing should be retained on the work agenda and that it would be premature to prioritize between the topics. The Commission confirmed its decision that the Working Group could take up work on those topics upon completion of the work on the Model Law on Electronic Transferable Records. The Commission requested the Secretariat, within its existing resources, and the Working Group to continue to update and conduct preparatory work on the two topics including their feasibility in parallel and in a flexible manner and report back to the Commission so that it could make an informed decision at a future session, including the priority to be given to each topic. In that context, it was mentioned that priority should be based on practical needs rather than on how interesting the topic was or the feasibility of work.[6]

6. At its fifty-fourth session (Vienna, 31 October-4 November 2016), the Working Group held a preliminary exchange of views on a possible future work on cloud computing. While no decision was made, it was noted that the preparation of a descriptive document listing issues relevant when reviewing contracts for cloud

[5] Ibid., *Seventieth Session, Supplement No. 17* (A/70/17), paras. 354, 356 and 358.
[6] Ibid., *Seventy-first Session, Supplement No. 17* (A/71/17), paras. 229-235.

computing services could be particularly useful in assisting small and medium-sized enterprises. It was added that such document should reflect contractual practices and, where available, legislation, and should refer to relevant technical standards, but should not have a legislative nature, without prejudice to future deliberations and decisions of the Commission (A/CN.9/897, para. 126).

7. As requested by the Commission (see para. 4 above), the Secretariat in this note shares with the Working Group results of the preparatory work accomplished so far in the area of cloud computing. The Secretariat is expected to report on those aspects to the Commission as well (see para. 5 above).

II. Results of preparatory work

A. Summary of steps taken by the Secretariat

8. The Secretariat used the proposals of Canada (A/CN.9/823 and A/CN.9/856; see paras. 1 and 3 above) as the basis for its preparatory work.

9. In addition to reviewing relevant reports, standards and publications, the Secretariat has undertaken informal consultations with experts. As broad participation in informal expert consultation as possible has been sought to ensure representation of views from all regions, principal economic and legal systems of the world and of developed and developing countries.

10. The Secretariat first sought comments from experts on the proposed outline of issues to be addressed in a text to be prepared by UNCITRAL or its secretariat in the area of cloud computing. The feedback received informed the structure and content of the text that was eventually circulated for comments by experts in the form of a draft legal guide on contractual aspects of cloud computing.

11. The draft legal guide elicited numerous comments, summarized in the sections below. There was consensus on many issues of technical nature and disagreement on some issues, mostly of policy nature, such as desirability and feasibility of preparing a detailed legal guide on contractual issues of cloud computing similar to existing UNCITRAL legal guides.[7] The policy issues summarized in section B below need to be resolved before any further preparatory work by the Secretariat in the area of cloud computing is undertaken. Sample chapters prepared by the Secretariat and annexed to this note are presented to the Working Group to facilitate the discussion of those issues.

B. Policy issues

1. Form of work

12. The consultations revealed preference for a non-legislative text that would analyse contractual issues relating to cloud computing and possible approaches to them. It was considered unfeasible and undesirable to prepare a legislative text (e.g. a model law or legislative guide) given sensitive policy issues, such as personal data protection and jurisdictional aspects, that cloud computing raised.

[7] See the *UNCITRAL Legal Guide on Drawing Up International Contracts for the Construction of Industrial Works* (1987), United Nations publication, Sales No. E.87.V.10 (A/CN.9/SER.B/2), available at www.uncitral.org/uncitral/en/uncitral_texts/procurement_infrastructure/1988Guide.html, and the *UNCITRAL Legal Guide on International Countertrade Transactions* (1992) referred to in paragraph 1 of this note.

13. Divergent views were expressed on the form of a possible non-legislative text. It was questioned whether legal issues arising from cloud computing contractual relationships were so distinct from other types of contracts, for example IT outsourcing, renting, services and licensing contracts, as to justify the preparation of a detailed legal guide on cloud computing akin to the existing UNCITRAL legal guides.[8] In addition, concern was expressed that a detailed legal guide could become quickly outdated in light of the rapid evolution of cloud computing contract practices.

14. Furthermore, in some jurisdictions cloud computing might be made subject to the principles applicable to public utilities (e.g. provision of safe and adequate service to all who apply for services without undue discrimination and for just and reasonable prices), which would considerably constrain the cloud services providers' freedom of contract. The value of a contractual legal guide in such cases would be doubtful.

15. The preparation of a short guidance text, which would be easier to agree upon and more user-friendly, was suggested. However, it was also stated that the length of a guidance text should be a secondary consideration since a text would need to be sufficiently detailed to provide useful guidance to contracting parties.

16. It was suggested that the main beneficiaries of a guidance text would be users of cloud computing services with a weaker bargaining position. It was therefore recommended that a guidance text should be prepared keeping that group of contracting parties in mind.

2. Scope of work and drafting approaches

17. Based on the understanding that, to remain relevant, a guidance text should avoid time-bound terms and concepts, a question was raised on whether a guidance text should nevertheless refer to existing types of cloud computing services (such as infrastructure as a service (IaaS), platform as a service (PaaS), etc.) and their deployment models (public, private, etc.). The unanimous view was that different types of services and different deployment models raised different legal issues and might justify different contract drafting approaches. It would therefore be unavoidable to describe in a guidance text the main characteristics of the existing types of cloud computing services and their deployment models. It was proposed that a guidance text should differentiate legal issues common to any cloud computing contract, regardless of the types of services involved and their deployment model, from those specific to a particular contract type.

18. Another question was whether it would be reasonable to expect that a guidance text could exhaustively deal with all legal issues arising from all possible types of cloud computing services (existing or future), their different deployment models and diverse business circumstances in which cloud computing contracts could operate. If not, restrain would need to be exercised in the choice of issues to be covered and the breadth and depth of their analysis in a guidance text, to make the project manageable. The text could for example focus only on data portability, interoperability, data breach, risks of multi-tenancy and other issues of most concern to contracting parties in cloud computing relationships.

19. The need to discuss issues of the general contract law if they do not raise any cloud-specific considerations was particularly questioned. Risks of intervening into the existing contract law framework and constraining the freedom of parties to contract by doing so were highlighted. Concern was also expressed about risks of touching upon issues of potentially regulatory concern: although a guidance text would not intend to provide guidance to policymakers considering the adoption of

[8] Ibid.

regulatory or legislative provisions dealing directly or indirectly with cloud computing services, a UNCITRAL text could nevertheless be considered reflecting a minimum internationally accepted standard of practice in contract dealings related to cloud computing services and thus a reference for good practice.

20. Another view was to adopt a more comprehensive approach, following examples of the existing UNCITRAL legal guides dealing with contract drafting issues.[9] The value of a more comprehensive guidance text for users in a weaker bargaining position was particularly highlighted.

21. Advisability of focusing on cloud-specific issues only in the business-to-business (B2B) context and excluding the business-to-consumer (B2C), government-to-business (G2B) and business-to-government (B2G) contexts was questioned. It was not clear from consultations whether, if the B2G context was to be covered,[10] a guidance text should provide any recommendations on such pre-tendering issues as the selection of a method or tool and award criteria for procurement of cloud computing services. (See the annex to this note for a sample chapter of a possible guidance text addressing specific legal issues arising from public cloud services contracts).

22. Views also differed on whether a guidance text should deal only with contracts between cloud service providers and cloud service customers or also cover contracts involving intermediaries, such as cloud services brokers or integrators. The extent of coverage of subcontracting issues was not clear either. Divergent views were also expressed on whether a guidance text should deal with sector-specific (e.g. healthcare or financial services) cloud services contracts. Neither was a common view on the extent of discussion of legal issues arising from possible infringement of third parties' rights (i.e. issues of privacy and personal data protection, consumer protection law) or from behaviour of users of cloud computing services other than the cloud services customer (e.g. the customer's employees).[11]

23. The careful assessment of risks arising from the use of cloud computing services before entering into binding commitments was considered particularly important. That assessment should cover not only contract performance but also post-contractual issues. The views however differed on whether a detailed legal guidance from UNCITRAL on pre-contractual due diligence would be feasible or desirable in light of the diverse factors that influence pre-contractual considerations. It was considered that a guidance text could highlight essential pre-contractual aspects, such as pre-contractual risk assessment, audits, service performance trials and verification of (sub)licensing status. Post-contractual issues would need to be discussed in detail in conjunction with relevant contractual clauses, such as on portability and export of data, post-contractual services, IP rights and post-contractual audits.

C. Possible contents and structure of a future text

24. In addition to the issues raised above and in the annexed sample chapters, the following issues, listed in a possible order of treating them, might be addressed in a chapter of a possible guidance text dealing with contract drafting aspects:

---

[9] Ibid.

[10] A related question is raised in document A/CN.9/823, para. 11: "Is the cloud computing and related legal issues different in the government context versus in the business context and should different standards apply?"

[11] Similar issues are raised in document A/CN.9/823, para. 8: "How are third parties and third parties-related information affected by cloud computing agreements?"

(a) *Freedom of contract and the applicable legal framework*: choice of law considerations specific to cloud computing, in particular how private international law would identify the governing law in the absence of parties' choice of law;[12]

(b) *Formation and form of the contract*: specifics of cloud services contract formation; and solutions for identification and authentication of the parties and users of cloud services (link to identity management and trust services);[13]

(c) *Description of services and performance parameters*: description of core, ancillary and optional services; explicit and implied warranties; consents and rights related to the performance of services; such service performance parameters as availability of services, response time, maintenance and upgrades; application of, and compliance with, technical standards; service performance monitoring and audits;[14]

(d) *Risk allocation*: description of risks in general and how to allocate them best in cloud services arrangements (e.g. data security, data protection and data breach risks). In that context, differing legal consequences may arise depending on the nature of the data placed on the cloud, the type of contract and other circumstances. Any minimum requirements for handling security and data breach would need to be discussed;[15]

(e) *Government access to data*: the extent to which a guidance text should address relationships of the contracting parties with government authorities in national or cross-border context would need to be clarified (e.g. reporting requirements to state agencies under data protection law, disclosure orders and

---

[12] Similar issues are raised in document A/CN.9/823, para. 10: "would a choice of applicable law and jurisdiction between the service provider and the service applicant pointing to State A validly oust jurisdiction of the national courts in State B where a user is located?"; and in document A/CN.9/856, para. 56: "where was the contract negotiated and signed in a virtual environment? Where is the contract expected to be performed? Where is the cloud computing service provider located?"; and ibid., para. 57: "should there be some guidance for cases where the parties accidentally or knowingly did not select a governing law? Should there be limits to the choice of governing law?"

[13] Similar issues are raised in document A/CN.9/823, para. 7: "is any contractual framework acceptable or should best practices be established [for identity management to ensure secured access to cloud data]? … how does States' domestic legislation apply to accepted identity management protocols? What do courts accept as reasonable practices and what do they consider being negligent practices?"

[14] Similar issues are raised in document A/CN.9/856, para. 65: "In the absence of any term in the contract for service, a person contracting to do work and supply materials warrants that the materials or services will be a sufficient quality and reasonably fit for the purpose for which they are contracted, unless the circumstances of the contract are such as to exclude any such warranty. Are there implied terms under a cloud contractual relationship? For example, does the cloud service provider warrant that it will comply with any applicable local laws where the data could be located? If the parties agree that the data should be hosted in specific geographic locations, does the cloud service provider warrant that it will be the case and that servers used for storage or computing purposes will be located exclusively in the designated jurisdiction?"

[15] Similar issues are raised in document A/CN.9/823, para. 6: "What duties does the service provider have towards preserving the integrity of the data? What remedies are available in cases where the integrity of the data has been compromised?" "…what duties does the service provider have in relation to business losses due to the unavailability of the service?"; and in document A/CN.9/856, para. 63: "What are the duties of the parties to a cloud computing agreement? Do they include the obligation to preserve data and redundancy? Are the parties limited to duties specifically mentioned in the cloud agreement? Do cloud service providers have the obligation to perform the contract according to recognized business practices and if so, what is the content of these practices?"; and ibid., para. 66: "Is it an implied term of the contract that the cloud provider is required to maintain control over data?"

preservation and production of evidence in criminal investigations and other contexts);[16]

(f) *IP issues*: proprietary licenses vs. open standards issues; limits on reproduction of content and communication to public; rights to applications that customers developed or deployed on the cloud; IP issues arising from modifications of the customer data; ownership rights on cloud-processed data (e.g. metadata); rights to improvements arising from the customer's suggestions; other scenarios of sharing IP; and intersection between IP developments and duty of care.[17] The extent to which a guidance text should discuss any IP issues would need to be clarified. Some experts echoed the already expressed views that IP issues should be excluded (see paras. 1 and 2 above). Others suggested highlighting in a guidance text risks of exploiting IP rights through cloud computing arrangements;

(g) *Price and payment*: mechanisms for price calculation and price adjustments; methods for measuring services;

(h) *Liability*: possible exemptions from, or limitations of, liability; remedies; damages; and liability insurance;[18]

(i) *Duration, renewal and termination*: fixed or indefinite duration; mechanisms for renewal; causes for termination; partial or complete termination; and handling of customer data upon termination.[19] The extent to which a guidance text should address the impact of insolvency of the cloud service provider or the customer on the cloud services contract would need to be clarified;

---

[16] Similar issues are raised in document A/CN.9/823, paras. 10 and 11: "should the host be subject to disclosure requirements even though it has very limited connection to the jurisdiction ordering disclosure?" and "Should the service provider be required to disclose that access to the data can be granted to a given State authority in the conduct of special investigative powers?" and in document A/CN.9/856, para. 61: "This clearly brings up the question of whether the encrypted information is subject to the other country's law and, if so, what practical effect this has. This practice raises the question of whether a court in the jurisdiction where the data is located may require the disclosure of the encryption key."; ibid., para. 62: "In civil and commercial matters, courts can issue an order for the production of documents actually in the possession and control of a party to the dispute. Should a cloud service provider be required to produce electronic documents falling under its control? If not, is domestic legislation providing clear guidance to that effect? Is this situation exacerbated in cross border situations?"

[17] Similar issues are raised in document A/CN.9/823, para. 8: "Who owns the data under these agreements?" and in document A/CN.9/856, para. 69: "In many systems of law, the public and peaceful possession of personal property amounts to a presumption of ownership. Does this presumption cause difficulties in the world of cloud computing? Is the cloud service provider in possession of the data of its customers? What happens in situations where the proprietary rights over data or software have not been clearly established by the parties to the cloud agreement in particular in situation where IA's is being supplied?"; ibid., para. 70: "Given the proprietary rights of customers over data maintained by the cloud service provider, should the service provider be required to surrender data to its legitimate owner upon demand? Would this obligation also include the obligation to erase or otherwise eliminate any back-up copies of the data?"

[18] Similar issues are raised in document A/CN.9/823, para. 11: "what practical and effective measures to limit risks should be put in place by service providers? For example should service providers be encouraged to offer multi-tiered access with varying access privileges (i.e., not all personal information about an entity is accessible to all users)? Should they be required to inform potential clients of the availability or unavailability of such safeguards and multi-tiered access functions? Should they contract liability insurance and who should be responsible for insuring a particular risk? … Is the existence of legislation on the protection of personal information and compliance by the service provider with the legislation sufficient to exonerate the provider from liability?"; and in document A/CN.9/856, para. 67: "Are limitations of liability for data losses or corruption enforceable or are they considered unconscionable or unenforceable because contrary to the purpose of the contract?"

[19] Similar issues are raised in document A/CN.9/823, para. 6: "Under what terms can a cloud agreement be terminated? What happens to the data when the contract is terminated?"

(j) *Amendments of contractual terms*: what would constitute amendments and what would be the result of routine maintenance and upgrades would need to be clarified; and

(k) *Dispute resolution*: alternative dispute resolution mechanisms, commercial arbitration and choice of jurisdiction considerations specific to cloud computing environment.[20] The extent of discussion of preventive injunctions, online dispute resolution issues and class and collective actions would need to be clarified.

25. The extent of relying on and reflecting in a guidance text cloud computing standards, such as those of the International Organization for Standardization (ISO), would need to be clarified.[21] For example, ISO standards in the area of cloud computing, elaborated in cooperation with other international organizations, do not only define cloud computing terms and provide technical standards in that area. They often contain guidance on what and how should be addressed in cloud services relationships.

III. Issues for consideration by the Working Group

26. The Working Group is expected to formulate recommendations for the consideration of the Commission on the feasibility and practical needs for the work on cloud computing, the exact scope of that work, possible methodology and priority to be allocated to that work (see paras. 4 and 5 above). In so doing, it may wish to address in particular:

(a) The form that a work product on cloud computing would take, i.e. whether a legal guide giving explanations concerning cloud services contract drafting, or another text would be prepared. In considering that aspect, the Working Group may wish to recall the diverse spectrum of texts that UNCITRAL has adopted, which could be broadly divided into: (i) legislative texts (conventions, model laws, legislative guides and recommendations, and model legislative provisions);[22] (ii) uniform

[20] Similar issues are raised in document A/CN.9/823, para. 10: "would a choice of applicable law and jurisdiction between the service provider and the service applicant pointing to State A validly oust jurisdiction of the national courts in State B where a user is located?"; and in document A/CN.9/856, para. 56: "For example, where was the contract negotiated and signed in a virtual environment? Where is the contract expected to be performed? Where is the cloud computing service provider located?"; ibid., para. 74: "What constitutes a sufficient connection to a given jurisdiction for a court to entertain a contractual claim arising out of a cloud computing agreement? To what extent should an exclusive choice of jurisdiction be recognized and enforced?"; and ibid., para. 75: "In the absence of a clause on jurisdiction where can the parties to the contract bring an action or seek provisional protection measures? What should be the basis for such exercise of jurisdiction?"

[21] Similar issues are raised in document A/CN.9/856, para. 33: "In recent years, the emergence of 'international standards' put forward by trade associations and non-governmental membership organizations have contributed to addressing and limiting legal risks associated with the Cloud. These standards are incorporated by reference in contracts between the cloud service provider and customers and represent an off-the-shelf solution to a number of cloud computing risks."; and ibid., para. 68: "The emergence of 'international standards' put forward by trade associations and non-governmental membership organizations may have contributed to addressing and limiting risks associated with the Cloud in particular for small and medium-sized enterprises which may not always have the resources or the expertise to consider all possible cloud-related issues. Should UNCITRAL consider whether such standards can be incorporated into best practices? Are these standards referred to in contracts between cloud service providers and customers effective and binding in the various systems of law?"

[22] Such UNCITRAL legislative texts as conventions and model laws are usually accompanied by explanatory materials (guides to enactment (and interpretation) or explanatory notes), prepared by UNCITRAL or its secretariat to assist with the use of the text. Explanatory materials are based on the records of the relevant legislative process in UNCITRAL. They may be adopted by the Commission (see e.g. the *Guide to Enactment of the Model Law on Public Procurement (Official*

contractual clauses and rules (such as the *UNCITRAL Arbitration Rules*[23]); and (iii) explanatory texts (such as legal guides, informational notes and recommendations);

(b) If a legal guide is to be prepared, whether it would be similar as regards the level of detail, arrangement and drafting approaches to the existing UNCITRAL legal guides,[24] or a different template would need to be followed;

(c) Scope of the work, in particular, whether a text to be prepared would purport to address all possible cloud computing contracts or only a particular group thereof or particular issues of cloud computing. Other important considerations related to the scope of the work and drafting approaches that the Working Group may wish to address are raised in paragraphs 17-23 above;

(d) The timing of the work in the area of cloud computing, i.e. whether the work should be undertaken before, after or in parallel with the work on the other topic assigned by the Commission to the Working Group (identity management and trust services); and

(e) A method of work, which is closely related to the preceding point. The Working Group may wish to make a recommendation to the Commission on whether the work should take place in the Working Group or in the Commission in plenary or handled by the Secretariat with the involvement of experts. In the latter case, the role of the Commission and the Working Group would need to be clarified. Different implications of the decision on a method of work on expert representation from States and on resources of the Secretariat necessary to provide substantive and conference management services should be taken into account.

27. In considering the most appropriate method of work, the Working Group may wish to recall that all legislative texts and most non-legislative texts were prepared by UNCITRAL either in a working group or at annual sessions of UNCITRAL. In their pre-adoption form, they were subject to comments by Governments and relevant international organizations. That was the case also with such non-legislative texts as the *UNCITRAL Legal Guide on Drawing up International Contracts for the Construction of Industrial Works*,[25] which was prepared by the Working Group on the New International Economic Order working on it from 1981 to 1987, and the *UNCITRAL Legal Guide on International Countertrade Transactions*,[26] whose draft chapters were prepared by the Secretariat and discussed in the Commission and in a working group from 1990 to 1992. Some non-legislative texts, although prepared by the UNCITRAL secretariat, were nevertheless subject to review and approval by UNCITRAL that authorized their publications as a product of the work of the Secretariat.[27]

Records of the General Assembly, Sixty-seventh Session, Supplement No. 17 (A/67/17), para. 46. The text of the Guide is available at www.uncitral.org/uncitral/en/uncitral_texts/procurement_infrastructure/2012Guide.html) or issued as a work product of the Secretariat (see e.g. the *Explanatory Note by the UNCITRAL secretariat on the 1985 Model Law on International Commercial Arbitration as amended in 2006* (United Nations publication, Sales No. E.08.V.4). Available at www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html).

[23] Available at www.uncitral.org/uncitral/en/uncitral_texts/arbitration/2010Arbitration_rules.html.

[24] See above, footnote 7.

[25] Ibid.

[26] See above, footnote 3.

[27] See e.g. the *UNCITRAL Legal Guide on Electronic Funds Transfers* (1987) (United Nations publication, Sales No. E.87.V.9 (A/CN.9/SER.B/1), available at www.uncitral.org/pdf/english/texts/payments/transfers/LG_E-fundstransfer-e.pdf), *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* (2007) (United Nations publication, Sales No. E.09.V.4, available at www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf), *UNCITRAL Practice Guide on*

28. Non-legislative texts vary significantly not only by subject but also by purpose, structure and presentation style. They may deal with issues not addressed in any other UNCITRAL text[28] or be linked to other UNCITRAL texts.[29] Reference to non-legislative texts in this context excludes explanatory materials that may accompany a UNCITRAL legislative text.[30]

Cross-Border Insolvency Cooperation (2009) (United Nations publication, Sales No. E.10.V.6, available at www.uncitral.org/uncitral/en/uncitral_texts/insolvency/2009PracticeGuide.html) and *Recognizing and Preventing Commercial Fraud: Indicators of Commercial Fraud* (2013) (see above, footnote 2).

[28] E.g. the *UNCITRAL Legal Guide on International Countertrade Transactions* (see above, footnote 3) is the only text of UNCITRAL on that subject. The same can be said about *Recognizing and Preventing Commercial Fraud: Indicators of Commercial Fraud* (2013) (see above, footnote 2).

[29] See e.g. *UNCITRAL Model Law on Cross-Border Insolvency: The Judicial Perspective* (2011) (available from www.uncitral.org/uncitral/uncitral_texts/insolvency.html); or *Recommendations to assist arbitral institutions and other interested bodies with regard to arbitration under the UNCITRAL Arbitration Rules as revised in 2010* (2012) (*Official Records of the General Assembly, Sixty-seventh Session, Supplement No. 17* (A/67/17), annex I).

[30] See above, footnote 22.

Annex

Sample chapters of a possible guidance text on contractual aspects of cloud computing, prepared by the Secretariat[31]

Introduction

Origin and Purpose

1. The guidance text covers cloud services contracts in which one party (the cloud service provider) provides to the other party (the customer) cloud services in the form of one or more capabilities via cloud computing. Capabilities may vary from the provision and use of simple connectivity and basic computing services (such as storage, emails, office applications) to the provision and use of the whole range of physical and virtual resources needed to build own information technology (IT) platforms, or deploy, manage and run customer-created or customer-acquired applications or software.

2. Cloud computing can generally be defined as supply and use of computing services (e.g., data hosting or data processing) through open or closed network. Cloud services contracts are thus a variation of contracts for provision of services. Depending on data involved in cloud computing, they could be subject to various legal regimes, inluding those on privacy protection, banking law and anti-money-laundering regulations. An international or cross-border dimension in this type of contracts is prevalent but cloud computing could be confined by law or practice to a single jurisdiction as well.

3. The Commission decided to undertake work in the area of cloud computing in recognition of a significant potential of cloud computing solutions for economic growth, in particular for small and medium enterprises (SMEs). [*to be elaborated drawing on future UNCITRAL records*]

…

4. The guidance text does not intend to express the position of UNCITRAL on the desirability of concluding cloud services contracts. It is intended merely to assist potential parties to a cloud services contract in identifying issues that they should consider before entering into, and while negotiating and drafting, a cloud services contract. The various solutions to issues discussed in the guidance text will not govern the relationship between the parties unless they expressly agree upon such solutions, or unless the solutions result from provisions of the applicable law.

5. The guidance text has been designed to be of use to persons regardless of their legal background. It is emphasized however that the guidance text should not be regarded by the parties as a substitute for obtaining legal and technical advice and services from competent professional advisers. Nor is the guidance text intended to be used for interpreting cloud services contracts.

6. The guidance text does not interfere with mandatory domestic rules; nor does it intend to provide a model for, or encourage the adoption, of special legislation on cloud computing. Apart from relevant local, national and international legal rules and the provisions of the contract, local, national and international standards or codes of practice may exist, which this guidance text does not purport to replace.

[31] The sample chapters do not reflect views of UNCITRAL or its working group. They are the result of the Secretariat's research and consultations with experts and also draw on documents A/CN.9/823 and A/CN.9/856. They presented in a draft form for consideration by the Working Group.

Scope of the guidance text

7. The guidance text highlights main considerations usually involved in concluding cloud services contracts regardless of the type of services and their deployment model. At the same time, the guidance text recognizes that cloud services contracts could take a variety of forms and display differing features depending upon the particular circumstances of the transaction. The guidance text highlights commonly encountered issues arising from particular types of cloud services and their deployment models [*to be confirmed*].

8. [The guidance text touches upon issues arising from the involvement of cloud service partners that may be engaged in support of, or auxiliary to, activities of either the cloud service provider or the customer or both. Examples of cloud service partners include cloud auditors and cloud service brokers. The guidance text addresses rights and remedies available to users of cloud services other than the customer (e.g. customers' clients, employees) only to a limited extent, in the context of possible clauses that could be considered for inclusion into a cloud service contract between the cloud service provider and the customer. [*The extent of coverage of third party aspects (subcontracting, brokers, auditors, rights of data subjects, consumers, other users of cloud services, etc.) in the guidance text is to be clarified.*]]

9. The guidance text may not be applicable to arrangements for the use of cloud services between cloud services providers and consumers to the extent that those arrangements would be subject to mandatory consumer protection law and regulations. [*Other exclusions from the scope, such as B2G, G2B, specific sectors, etc., are to be discussed.*]

10. Cloud computing and cloud services could involve cross-border operations or could be confined to a particular region or country. This guidance text could be used by the parties regardless of a cross-border factor. For most standardized simple cloud services, that factor would not matter; under some circumstances, cross-border aspects may add an additional layer of complexity discussed in this guidance text.

11. The guidance text is not dealing with issues of licensing and outsourcing arrangements although some aspects of cloud services may resemble those relationships.

Arrangement of the guidance text

12. The guidance text is arranged in several parts. The first part introduces a reader to contracts covered by the guidance text and benefits and risks of cloud computing. The second part deals with certain matters arising prior to the time when the contract is drawn up and describes possible contracting approaches to structuring a cloud services contract depending on the type and deployment model chosen by the contracting parties. The discussion of these subjects has two aims: to direct the attention of the parties to important matters which they should consider prior to commencing the negotiation and drawing up of a cloud services contract, and to provide a setting for the discussion of the legal issues involved in the contract.

13. The third part discusses possible types of contract clauses that parties may use. The discussion in the guidance text is restricted to those types of clauses that are specific to or of special importance for cloud computing services. Some of the clauses described in the guidance text are essential for concluding a cloud services contract. Other clauses discussed in the guidance text may be useful in the context of the particular commercial circumstances, in particular in the light of the type of services and their deployment model. Throughout the guidance text, whenever appropriate, the discussion points out that different solutions may apply under different contracting approaches. In view of the great variety of circumstances in which cloud services

contracts are concluded, the guidance text does not contain a general suggestion as to the types of clauses that parties should agree upon. It is for the parties to each contract to judge the extent to which the issues considered in the guidance text are relevant to their contract.

14. [The last part deals with specific legal issues that cloud services contracts raise in the G2B and B2G contexts and in sectors subject to special regulation, such as healthcare and financial services.] [*to be confirmed*]

Approach to drafting

15. Given its purpose to help contracting parties to identify pitfalls, limitations and other difficulties in the negotiation or execution of cloud services contracts, recommendations are made in the guidance text aimed at suggesting ways in which certain issues in a cloud services contract might be settled. Three levels of suggestion are used. The highest level is indicated by a statement to the effect that the parties "should" take a particular course of action. It is used sparingly in the guidance text and only when a particular course of action is a logical or legal necessity. An intermediate level is used when it is "advisable" or "desirable", but not logically or legally required, that the parties adopt a particular course of action. The lowest level of suggestion is expressed by formulations such as "the parties may wish to consider" or "the parties might wish to provide" or the agreement by the parties "might" contain a particular solution. The wording used for a particular suggestion may be, for drafting reasons, varied somewhat from that just indicated; however, it should be clear from the wording what level of suggestion is intended.

16. Since a prevailing terminology has been developed by various international and regional institutions active in the area of cloud computing, including the International Organization for Standardization (ISO), the guidance text uses the established terminology for the purpose of ensuring consistency, harmonization and legal clarity.

Part One. Cloud services contracts

Distinct features of cloud services contracts[32]

17. Distinct features common for all cloud services contracts are derived from the following typical characteristics of cloud computing via which the cloud services are provided:

(a) **Broad network access** means that capabilities can be accessed over the network from any place where the network is available (e.g. through Internet), using a wide variety of devices, such as mobile phones, tablets and laptops;

(b) **Measured service** means metered delivery of cloud services like in public utilities sector (gas, electricity, etc.), allowing monitoring the usage of the resources and charging by usage (on a pay-as-you-go basis);

(c) **Multi-tenancy** means that physical and virtual resources are allocated to multiple users whose data is isolated and inaccessible to one another;

(d) **On-demand self-service** means that services are used by the customer as needed, automatically or with minimal interaction with the cloud service provider;

(e) **Rapid elasticity and scalability** means the capability for rapid scaling, up or down, of the access or services provided in accordance with customer's requirements;

[32] ISO/IEC 17788: 2014 and document A/CN.9/856 were used for drafting this section.

(f) **Resource pooling** means that physical or virtual resources can be aggregated by the cloud service provider in order to serve one or more customers without their control or knowledge over the processes involved.

18. There are various ways in which cloud computing can be organized based on the control and sharing of physical or virtual resources (deployment models), including:

(a) **Community cloud** where cloud services exclusively support a specific group of related cloud service customers with shared requirements, and where resources are controlled by at least one member of that group;

(b) **Private cloud** where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer;

(c) **Public cloud** where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider;

(d) **Hybrid cloud** using at least two different cloud deployment models.

19. The extent of management and control by the customer of resources provided under the cloud services contract would depend on the type of capabilities provided to the customer and the cloud deployment model. In some cases, the customer would not manage or control the underlying physical and virtual resources, but would have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls). In other cases, the customer would not have any control over the resources other than devices connecting it to the network.

Benefits and risks[33]

20. The economic benefits of using cloud computing arise from economy of scale achieved by pooling computing resources within the control of one cloud service provider who then offers them at discounted prices to multiple customers. The economic benefits at the microeconomic level may produce the positive impact at a macroeconomic level on businesses and international trade.

21. Reduced need for the capital investment in IT infrastructure and savings of operational costs associated with IT governance are cited among attractive features of cloud computing especially for start-ups and SMEs. Another important consideration is access to enhanced IT security, specialized staff, increased data storage capacity, improved data preservation and other state-of-the-art computing services features. Cloud computing may also be more user friendly than traditional IT services and allow for more flexibility, productivity and innovation.

22. At the same time, cloud computing is not risk-free. It involves outsourcing and associated risks. Financial losses may result from incomplete or inaccurate assessment of business needs, cloud computing risks and potential cost savings. They may also result from business interruption or loss of revenues because of reputational damage.

23. Specific cloud computing risks stem in particular from:

(a) **Loss of control**. The customer's decision to migrate all or part of its activities and data to cloud computing leads to the loss of exclusive control over them. The extent of the loss of control depends on the type of cloud service. The customer's ability to deploy the necessary measures to guarantee data integrity and confidentiality or verify whether data processing and retention are being handled adequately may be particularly affected;

[33] Document A/CN.9/856 was used for drafting this section.

(b) **Inherent features of cloud computing**. Inadequate security practices of the cloud service provider will raise risks for the customer. They may relate to inadequate silo architecture, isolation of resources and data segregation, insufficient identity management procedures, and the absence of special precautions to prevent attacks on the cloud computing infrastructure. Such inherent features of cloud computing as multi-tenancy and virtualization may exacerbate security risks;

(c) **Remote access to services** that provides opportunities for cyber attacks such as interception of communications, including passwords, phishing, fraud and the exploitation of software vulnerabilities;

(d) **Cross-border data flows**. Protecting personal and other sensitive data as well as respecting the right to privacy is particularly difficult in infrastructures that are shared and potentially accessible to governments. The lack of information about the location of the data and the number of stakeholders involved in the provision of cloud computing services accentuates data breach risks;

(e) **The loss or compromise of credentials for access to cloud computing services**, which is one of the common causes of data loss or data disclosure to unauthorized persons;

(f) **Vagueness in sharing roles and responsibilities**. Various stakeholders are involved in a cloud solution model: the cloud service provider, the customer, third parties whose information is held by the customer, etc. Any ambiguity in defining the roles and responsibilities related to data ownership, access control, maintenance of infrastructure, etc. may result in security and other risks. The failure to clearly assign responsibilities will have a higher impact where a third party's IT resources are used.

[Part two. Pre-contractual aspects]

[*the extent of discussion, if any, of relevant issues in the guidance text is to be clarified*]

…

Part three. Contract drafting

…

[*for possible contents of this chapter, see paragraph 24 of the main part of this note*]

[Part four. Specific legal issues of cloud services contracts in … [*areas, if any, are to be identified*]

[*Below is a sample chapter prepared by the Secretariat to illustrate a possible approach to drafting chapters on specific legal issues that cloud services contracts raise in contexts other than the B2B context and in sectors subject to special regulation, such as healthcare and financial services. The B2G context is used for illustration.*

If B2G transactions are to be covered in a guidance text, the list of issues set out below is for consideration by the Working Group. In addition, it is to be decided whether any guidance should be provided on such pre-contractual issues as defining specifications or performance requirements and selection of the appropriate procurement method or tool.]

Public cloud services contracts

24. Public entities entering into a cloud service contract would face similar issues about service performance levels, data security, protection and privacy to those discussed in the context of business-to-business (B2B) contracts. Additional or distinct complexities would arise because of the public nature of customers of cloud services and the role of public entities in implementing a public procurement function and socio-economic policies of a State.

25. Usually public entities are subject to various layers of laws that are not applicable to private entities, such as on freedom of information, State records and State archives, public queries, investigation, etc. Those laws would become applicable to cloud service providers by virtue of their contractual relationships with a public entity. Public entities and their employees would nevertheless remain subject to criminal, civil and administrative liability for the failure to exercise properly public functions entrusted to them, including if public data placed on the cloud containing protected information (e.g. classified information, personally identifiable information, commercially sensitive information) is misused or erroneously disclosed. The reputation of the government and public trust will thus be closely tied to the quality of cloud services.

26. Statutory requirements applicable to public entities may in particular dictate:

(a) With whom a public contract for cloud services could be concluded (cloud service providers may need to be certified by State agencies or there could be limits to contract with foreign entities);

(b) Which data could be migrated to cloud platforms (the move of data of a sensitive nature to the cloud may be prohibited);

(c) Under which terms and according to which standards cloud services could be used (law may dictate higher standards for security, privacy, confidentiality, accessibility, authentication, continuity of service, interoperability and portability, data breach notification obligations, restrictions on the geographical location of data in motion and data at rest and data centres, servers and redundant servers);

(d) Special rules on subcontracting. The advance consent of the procuring entity may be required for any subcontracting that was not announced in tender documents. No blanket consent for subcontracting would be acceptable since this could interfere with the principles of good governance and competition (unchecked subcontracting may promote collusion). There could be therefore mandatory verification of subcontractors and the obligation to replace the existing ones if compulsory grounds for that exist. In addition, it is common for subcontractors to be subject to the same terms of procurement as those imposed on the main contractor. The cloud service provider would therefore be required to reflect those terms in any existing or future subcontracting arrangements;

(e) Warranties, adequate capital or insurance coverage to be provided by the cloud service provider;

(f) Mandatory training for the cloud service provider’s personnel handling sensitive information;

(g) State records management rules, in particular features allowing e-discovery and evidence preservation, the obligation to retain public data and related metadata in a certain form, including after the contract, disposition of records according to the State approved record schedules, and transfer of permanent records to the State archive in a prescribed form;

(h) Other additional functionalities, such as for implementing social policies of a State, e.g. accessibility of public data to disabled, and for interacting with individuals and legal entities, e.g. adherence to statutory deadlines for actions.

27. Public entities may also face significant restrictions on their ability to indemnify cloud service providers, agree on some dispute resolution clauses (e.g. on arbitration or jurisdiction of a foreign State) and accept click-through arrangements. They may also be required to include non-disclosure provisions and modify such standard clauses usually found in standard cloud services contracts in the B2B and business-to-customer (B2C) environments as broad downtime or other rights of cloud service providers, the absence of liability of cloud service providers for service failures and no obligation to indemnify customers in such cases. They may also be required to ensure that contractual clauses prohibit the cloud service provider from using the data for any of the providers' own purposes (such as advertising or other commercial activities). They would also not be able to agree on the transfer of any intellectual property (IP) ownership to the provider in any data stored on behalf of the public entity.

28. Grounds for termination by the Government of the contract in the business-to-government (B2G) context could also be broader, including for convenience. Law may also require termination of the contract by a public entity for corruption, fraud and other reasons specified in law and impose unlimited liability of a cloud service provider in such cases.

29. Procuring entities must be aware of any statutory requirements applicable to a cloud service contract in question. Those requirements may vary depending on the type of services to be provided and deployment model. Specifics of procurement of on-demand services as opposed to fixed price purchases would also need to be considered in light of State budgeting processes. All those issues would dictate approaches to formulating eligibility, qualification, examination and evaluation criteria and selecting the most appropriate method or tool for procurement of required cloud computing services. They would therefore need to be considered at the procurement planning stage.

30. Carefully considering all those issues already at the procurement planning stage is especially important for public procuring entities since, unlike private entities, they would not have much freedom to negotiate the terms of the contract at the stage of the conclusion of the contract and to renegotiate contractual terms in response to problems at the contract implementation stage. The public procurement contract would have to incorporate the terms and conditions of the procurement as specified in the solicitation documents at the outset of the procurement and as set out in the terms and conditions of the winning tender. Any material changes to those terms and conditions at the conclusion of the contract or during its implementation would violate the key principles of transparency, competition and objectivity in public procurement. Any changes that would affect the nature of the contract, the pool of potential participants in the procurement proceedings or the result of the selection would be considered material. The right of the cloud service provider to unilaterally change the terms of the contract, often included in standard cloud services contracts in the B2B and B2C environments, would therefore need to be substantially modified, if not excluded altogether.]