United Nations A/CN.9/WG.IV/WP.148*

General Assembly

Distr.: Limited
30 January 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-sixth session
New York, 16–20 April 2018

Contractual aspects of cloud computing

Note by the Secretariat

Contents

* Reissued for technical reasons on 13 March 2018.

V.18-00389 (E)

I. Introduction

1. The Working Group may wish to refer to paragraphs 1 to 6 of document A/CN.9/WG.IV/WP.142 for background information related to its work on cloud computing until the fifty-fifth session of the Working Group (New York, 24–28 April 2017). A summary of developments related to that work in the Working Group at its fifty-fifth session and in the Commission at its fiftieth session may be found in the provisional agenda of the current session (see document A/CN.9/WG.IV/WP.147, paras. 7 and 8).

2. In accordance with the recommendation of the Working Group for possible future work on cloud computing (A/CN.9/902, para. 23) and views expressed in the Commission at its fiftieth session on the same matter,[1] the Secretariat submits a draft checklist of main issues of cloud computing contracts to the Working Group for its consideration. The draft checklist, prepared by the Secretariat with the involvement of experts, reflects the preliminary considerations of the Working Group as regards the scope and contents of, and approaches to drafting, a checklist (A/CN.9/902, paras. 11–28).

3. The Working Group is expected to report on progress of its work on cloud computing to the Commission at its fifty-first session (New York, 25 June–13 July 2018).[2] In the light of intended users of a checklist and of transactions for which it is expected to be used, the Working Group may wish to consider whether the checklist should be prepared as an online reference tool. If so, the Working Group may wish to recommend that course of action to the Commission, in particular that the Secretariat should prepare an online reference tool that would reflect the substantive content of the draft checklist as revised by the Working Group at its fifty-sixth session and the Commission at its fifty-first session.

II. Draft checklist of main issues of cloud computing contracts

[*The terms appearing in bold throughout the checklist are described in the glossary in the end of the checklist. In an online reference tool they may be explained in a more user-friendly way.*]

Introduction

1. The checklist addresses main issues of cloud computing contracts between business entities where one party (the provider) provides to the other party (the customer) one or more **cloud computing services** for the end use. Contracts for resale or other forms of further distribution of **cloud computing services** are excluded from the scope of the checklist. Also excluded from the scope of the checklist are contracts with **cloud computing service partners** and other third parties that may be involved in the provision of the cloud computing services to the customer (e.g., contracts with sub-contractors and Internet service providers).

2. Cloud computing contracts may be qualified under the applicable law as a service, rental, outsourcing, licensing, mixed or other type of contract. Statutory requirements as regards its form and content may vary accordingly. In some jurisdictions, parties themselves in their contract may qualify the contract as a contract of a particular type if legislation is silent or vague on that issue; the court would take such qualification into account in interpreting the terms of the contract unless this would contradict the law, court practice, the actual intention of the parties, factual situation or business customs or practices.

[1] *Official Records of the General Assembly, Seventy-second Session, Supplement No. 17* (A/72/17), paras. 116–127.

[2] Ibid., paras. 116 and 127.

3. The issues addressed in this checklist may arise from cloud computing contracts regardless of the type of **cloud computing services** (e.g., **IaaS, PaaS or SaaS**), their **deployment model** (e.g., public**, community, private or hybrid)** and payment terms (with or without remuneration). The primary focus of the checklist is on contracts for provision of **public SaaS**-type cloud computing services for remuneration.

4. Ability to negotiate cloud computing contract clauses would depend on many factors, in particular on whether the contract involves **standardized commoditized multi-subscriber cloud** solutions or an individual tailor-made solution, whether a choice of competing offers exists, and on the bargaining positions of the potential parties. The ability to negotiate terms of a contract, in particular clauses on unilateral suspension, termination or modification of the contract by the provider and liability clauses, may be an important factor in choosing the provider where the choice exists [cross-link]. Having been prepared primarily for parties negotiating a cloud computing contract, the checklist may nevertheless also be useful for customers reviewing standard terms offered by providers to determine whether those terms sufficiently address the customer's needs.

5. The checklist should not be regarded by the parties as an exhaustive source of information on drafting cloud computing contracts or as a substitute for obtaining any legal and technical advice and services from competent professional advisers. The checklist suggests issues for consideration by potential parties before and during contract drafting without intending to convey that all of those issues must always be considered. The various solutions to issues discussed in the checklist 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. Headings and sub-headings used in the checklist and their sequence are not to be regarded as mandatory or suggesting any preferred structure or style for a cloud computing contract. The form, content, style and structure of cloud computing contracts may vary significantly reflecting various legal traditions, drafting styles, legal requirements and parties' needs and preferences.

6. [The checklist is not intended to express the position of UNCITRAL on the desirability of concluding cloud computing contracts.]

7. The checklist consists of two parts and a glossary: part one addresses main pre-contractual aspects that potential parties, primarily the customer, may wish to consider before entering into a cloud computing contract; part two addresses main contractual issues that negotiating parties may face while drafting a cloud computing contract; and the glossary describes some technical terms used in the checklist, to facilitate understanding.

Part One. Main pre-contractual aspects

A. Verification of mandatory law and other requirements

8. The legal framework applicable to the customer, the provider or both may impose conditions for entering into a cloud computing contract. Such conditions may stem also from contractual commitments, including **intellectual property (IP) licences**. The customer and the provider should in particular be aware of laws and regulations related to **personal data**, cybersecurity, export control, customs, tax, trade secrets, IP and **sector-specific regulation** that may be applicable to them and their future contract. Negative consequences of noncompliance with mandatory requirements may be significant, including, invalidity or unenforceability of a contract or part thereof, administrative fines and criminal liability.

9. Conditions for entering into a cloud computing contract may vary by sector and jurisdiction. They may include requirements to take special measures for protection of **data subjects' rights,** to deploy a particular model (e.g., **private** as opposed to **public cloud**), to encrypt data placed in the cloud and to register a transaction or a software used in the processing of **personal data** with State authorities. They may also include **data localization** requirements, as well as requirements regarding the provider.

- *Data localization*

10. **Data localization** requirements may in particular arise from the law applicable to personal **data**, accounting data and public sector data and export control laws and regulations that may restrict the transfer of certain information or software to particular countries. They may also arise from contractual commitments, e.g., **IP licences** that may require the licensed content to be stored on the user's own secured servers. **Data localization** may be preferred for purely practical reasons, for example to increase **latency**, which may be especially important for real-time operations, such as stock exchange trading.

11. Providers' standard terms may expressly reserve the right of the provider to store customer data in any country in which the provider or its sub-contractors do business. Such a practice will most likely be followed even in the absence of an explicit contractual right, since it is implicit in the provision of **cloud computing services** that they are provided, as a general rule, from more than one location (e.g., back-up and antivirus protection may be remote and support may be provided in a global "**follow-the-sun**" model). The customer that must comply with **data localization** requirements would need assurances from the provider that those requirements can be met. Where negotiation of a cloud computing contract is possible, contractual safeguards may be included, such as prohibition of moves outside the specified location or a requirement that the provider seek the prior approval of the customer for such moves [cross-link].

- *Requirements as regards the provider*

12. The customer's choice of a suitable provider may be restricted, in addition to market conditions, by statutory requirements. There may be a statutory prohibition to enter into a cloud computing contract with foreign providers, providers from certain jurisdictions or providers not accredited/certified with competent State authorities. There may be a requirement for a foreign provider to form a joint venture with a national provider or to acquire local licenses and permissions, including export control permissions, for the provision of **cloud computing services** in a particular jurisdiction. **Data localization** requirements [cross-link] may also influence the choice of a provider. In choosing a suitable provider, the customer may also be concerned with any statutory obligations on the provider to disclose or provide access to the customer data and other content to State authorities of foreign States.

B. Pre-contractual risk assessment

13. The applicable mandatory law may require risk assessment as a pre-condition to enter into a cloud computing contract. Even in the absence of statutory requirements, potential parties to a cloud computing contract may decide to undertake risk assessment that might help them to identify appropriate risk mitigation strategies, including negotiation of appropriate contractual clauses.

14. Not all risks arising from cloud computing contracts would be cloud specific. Some risks would need to be handled outside a future cloud computing contract (e.g., risks arising from online connectivity interruptions) and not all risks could be mitigated at an acceptable cost (e.g., reputational damage). In addition, risk assessment would not be a one-off event before concluding a contract. Risk assessment could be ongoing during the operation of the contract, and risk assessment outcomes may necessitate amendment or termination of the contract.

- *Verification of information about the chosen provider*

15. The following information may inform the customer about possible risks of dealing with a particular provider:

(a) The privacy, confidentiality and security policies of the provider, in particular as regards prevention of unauthorized access, use, alteration or destruction of the customer's data during processing, transit or transfer into and out of the provider's system;

(b) Assurances of the customer's ongoing access to **metadata,** audit trails and other logs demonstrating security measures;

(c) The existing disaster recovery plan and notification obligations in the case of a security breach or system malfunction;

(d) Migration-to-the-cloud and end-of-service assistance offered by the provider and provider's assurances of **interoperability** and **portability**;

(e) The existing measures for vetting and training of employees, sub-contractors and other third parties involved in the provision of the cloud computing services;

(f) Statistics on security incidents and information about past performance with disaster recovery procedures;

(g) Certification by an independent third party on compliance with technical standards;

(h) Evidence of regularity and extent of audit by an independent body;

(i) Financial standing;

(j) Insurance policies;

(k) Possible conflicts of interest; and

(l) Extent of sub-contracting and **layered cloud computing services**.

- *Penetration tests, audits and site visits*

16. Laws and regulations mandatorily applicable to the customer may require **audits**, penetration tests and physical inspection of data centres involved in the provision of the cloud computing services, in particular to ascertain that their location complies with statutory **data localization** requirements. The customer and the provider would need to agree on conditions for undertaking those activities, including their timing, allocation of costs and indemnification for any possible damage caused to the provider as a result of those activities.

- *IP infringement risks*

17. IP infringement risks may arise if, for example, the provider is not the owner or developer of the resources that it provides to its customers, but rather uses them under a **IP licence** arrangement with a third party. IP infringement risks may also arise if the customer is required, for the implementation of the contract, to grant to the provider a licence to use the content that the customer intends to place in the cloud. In some jurisdictions, storage of the content on the cloud even for back-up purposes may be qualified as a reproduction and require prior authorization from the IP rights owner.

18. It is in the interests of both parties to ensure beforehand that the use of the cloud computing services would not constitute an infringement of IP rights and a cause for the revocation of the IP licences granted to either of them. Costs of IP infringement may be very high. The right to sub-licence may need to be arranged, or a direct licence arrangement may need to be concluded with the relevant third-party licensor under which the right to manage the third party licences will be granted. The use of open source software or other content may necessitate obtaining an advance consent from third parties and disclosing the source code with any modifications made to open source software or other content.

- *Lock-in risks*

19. Avoiding or reducing **lock-in** risks may be one of the most important considerations for the customer. **Lock-in** risks may arise in particular from the lack of **interoperability** and **portability.** The law may not require the provider to ensure **interoperability** and **portability**. The onus might be completely on the customer to create compatible export routines, unless the contract provides otherwise.

20. The contract may in particular contain the provider's assurances of **interoperability** and **portability**. It may require the use of common, widely used standardized or interoperable export formats for data and other content or give the customer the right to choose among available formats. The contract may also need to address the customer's rights to joint products and the provider's applications or software, without which the use of customer data and other content in another cloud host or in-house may be impossible [cross-link]. The contract may also include the provider's obligations to assist with the export of customer data back in-house or to another provider upon termination of the contract [cross-link]. The customer would also need to carefully consider the impact of the duration of the contract: higher lock-in risks may arise from long-term contracts and from automatically renewable short- and medium-term contracts [cross-link].

21. The customer may consider testing beforehand whether data and other content can be exported to another cloud provider or back in-house and made usable there. It may also need to ensure synchronization between cloud and in-house platforms and replication of its data elsewhere. Transacting with more than one provider and opting for a combination of various types of **cloud computing services** and their **deployment models** (i.e., multi-sourcing), although possibly with cost and other implications for the customer, may be an important mitigating strategy against **lock-in** risks.

- *Business continuity risks*

22. The customer would be concerned about business continuity risks not only in anticipation of the scheduled termination of the contract, but also its possible earlier termination, including when either party may no longer be in business. Business continuity risks may also arise from the provider's suspension of the provision of the cloud computing services. The customer may be required by law to have an appropriate strategy planned in advance in order to ensure business continuity and avoid the negative impact of termination or suspension of the cloud computing services on end-users. Contractual clauses may assist the customer with mitigating business continuity risks, in particular in case of the provider's insolvency [cross-link] and unilateral suspension or termination of the cloud computing services [cross-link].

- *Exit strategies*

23. The customer would need to consider ahead of time the content that will be subject to exit (e.g., only the data that the customer entered in the cloud or also **cloud service derived data**). The customer would also need to seek assurances of its timely access to any decryption keys kept by the provider or third parties. It would also need to think about any amendments that would be required to **IP licenses** to enable the use of data and other content outside the provider's system. Where the customer has developed programs to interact with the provider's application programming interfaces (API) directly, they may need to be re-written to take into account the new provider's API. **SaaS** customers with a large user-base can incur particularly high switching costs when migrating to another **SaaS** provider, as end-user re-training would be necessary.

24. All those factors and the time frame that would be needed to export and make fully usable all customer data and other content back in-house or in another provider's system would need to be taken into account in negotiating end of service contractual clauses [cross-link].

C. Other pre-contractual issues

- *Disclosure of information*

25. The applicable law may require potential parties to a contract to provide each other with information that would allow them to make an informed choice about the conclusion of the contract. In some jurisdictions, the absence, or the lack of clear communication to the other party, of any information that would make the object of the obligation determined or determinable prior to contract conclusion may make a contract or part thereof null and void or entitle the aggrieved party to claim damages.

26. In some jurisdictions, the pre-contractual information may be considered an integral part of the contract. In such cases, the parties would need to ensure that such information is appropriately recorded and that any mismatch between that information and the contract itself is avoided. The parties would also need to deal with concerns over the impact of pre-contractually disclosed information on flexibility and innovation at the contract implementation stage.

- *Confidentiality*

27. Some information disclosed at the pre-contractual stage may be considered confidential (e.g., security, identification and authentication required by the customer or offered by the provider, information about sub-contractors and information about the location and type of data centres, which in turn may identify the type of data stored there and access thereto by State authorities, including of foreign States). Potential parties may need to agree on confidentiality of information to be disclosed at the pre-contractual stage. Written confidentiality undertakings or non-disclosure agreements may be required also from third parties involved in pre-contractual due diligence (e.g., auditors).

- *Migration to the cloud*

28. Before migration to the cloud, the customer would usually be expected to classify data to be migrated to the cloud and secure it according to its level of sensitivity and criticality and inform the provider about the level of protection required for each type of data. The customer may also need to supply to the provider other information necessary for the provision of the services (e.g., the customer's data retention and disposition schedule, user identity and access management mechanisms and procedures for access to the encryption keys if necessary).

29. In addition to the transfer of data and other content from the customer or customer's previous provider to the provider's cloud, migration to the cloud may involve installation, configuration, encryption, tests and training of the customer's staff and other end-users. The provider may agree to help the customer with those

issues, for extra fees or otherwise, as part of the contract with the customer or under a separate agreement with the customer or a third party acting on behalf of the customer (e.g., **a system integrator**). Parties involved in the migration would need to agree on their roles and responsibilities as regards installation and configuration, the format in which the data or other content is to be migrated to the cloud, timing of migration, an acceptance procedure to ascertain that the migration was performed as agreed and other details of the migration plan.

Part Two. Drafting a contract

A. General considerations

- *Freedom of contract*

30. The widely recognized principle of freedom of contract in business transactions allows parties to enter into a contract and to determine its content. Restrictions on freedom of contracts may stem from legislation on non-negotiable terms applicable to particular types of contract or rules that punish abuse of rights and harm to public order, morality and so forth. The consequences of non-compliance with those restrictions may range from unenforceability of a contract or part thereof to civil, administrative or criminal liability. Enforceability of contracts not freely negotiated, especially those that impose abusive terms on a party in a weaker bargaining position [cross-link], may in particular be questionable in jurisdictions where parties are expected to respect the principles of good faith and fair dealing.

- *Contract formation*

31. The concepts of offer and acceptance have traditionally been used to determine whether and when the parties have reached an agreement as regards their respective legal rights and obligations that will bind them over the duration of the contract. The applicable law may require certain conditions to be fulfilled for a proposal to conclude a contract to constitute a final binding offer (e.g., the proposal is to be sufficiently definite as regards the covered cloud computing services and payment terms).

32. The contract is concluded when the acceptance of the offer becomes effective. There could be different acceptance mechanisms (e.g., for the customer clicking a check box on a web page, registering online for a cloud computing service, starting to use cloud computing services or paying a service fee; for the provider starting or continuing to provide services; and for both parties signing a contract online or on paper). Material changes to the offer (e.g., as regards liability, quality and quantity of the cloud computing services to be delivered or payment terms) may constitute a counter-offer that may need to be accepted by the other party for a contract to be concluded.

33. **Standardized commoditized multi-subscriber cloud solutions** are as a rule offered through interactive applications (e.g., “click-wrap” agreements). There may be no or very little room for negotiating and adjusting the standard offer. Clicking “I accept”, “OK” or “I agree” is the only step expected to be taken to conclude the contract. Where negotiation of a contract is involved, contract formation may consist of a series of steps, including preliminary exchange of information, negotiations, delivery and acceptance of an offer and the contract’s preparation.

- *Contract form*

34. Cloud computing contracts are typically concluded online. They may be called differently (a cloud computing service agreement, a master service agreement or terms of service (TOS)) and may comprise one or more documents such as an **acceptable use policy (AUP)**, a **service level agreement (SLA)**, a data processing agreement or data protection policy, security policy and license agreement.

35. The legal rules applicable to cloud computing contracts may require that the contract be in **writing**, especially where **personal data processing** is involved, and that all documents incorporated by reference be attached to the master contract. Even when **written** form is not required, for ease of reference, clarity, completeness, enforceability and effectiveness of the contract, the parties may decide to conclude a contract in **writing** with all ancillary agreements incorporated thereto.

36. The signing of a contract on paper may be required under the applicable law, e.g., for tax reasons in some jurisdictions.

- *Definitions and terminology*

37. Due to the nature of **cloud computing services**, cloud computing contracts would by necessity contain many technical terms. The glossary of terms may be included in the contract as well as definitions of main terms used throughout the contract, to avoid ambiguities in their interpretation. The parties may wish to consider using the internationally established terminology for the purpose of ensuring consistency and legal clarity.

- *Minimum contract content*

38. A contract would normally: (a) identify the contracting parties; (b) define the scope and object of the contract; (c) specify rights and obligations of the parties, including payment terms; (d) establish the duration of the contract and conditions for its termination and renewal; and (e) identify remedies for breach and exemptions from liability. It usually also contains dispute resolution and choice of law and choice of forum clauses.

B. Identification of contracting parties

39. Correct identification of contracting parties may have a direct impact on the formation and enforceability of the contract. The name of the legal person, its legal form, business registration number (if applicable), and registered office or business address, together with statutory documents of that legal person usually provide a sufficient basis for ascertaining the legal personality of a business entity (be it a company or an individual) and its capacity to enter into a binding contract. The law may require additional information, for example an identification number for tax purposes or power of attorney to ascertain the power of a natural person to sign and commit on behalf of a legal entity.

40. Verification of the identity of a legal person may be carried out in various ways either directly by the parties or by relying on a third party. Parties are usually free to determine methods of identification unless the applicable law prevents them from doing so. The physical presence of an authorized representative of the legal person may be required, or the remote presence using electronic identification means acceptable to the parties may be sufficient. Where parties can choose, their choice is usually dictated by several factors, including risks involved in a particular contractual dealing. Some legislation may require or recognize only some methods of identification, in particular for issuing a power of attorney. It may also require the provider to identify its customers to competent State authorities in accordance with applicable standards.

C. Defining the scope and the object of the contract

41. Objects of cloud computing contracts vary substantially in their type and complexity given the range of **cloud computing services**. Within the duration of a single contract, the object may change: some **cloud computing services** may be cancelled and other services may be added. The object of the contract may comprise the provision of core, ancillary and optional services.

42. Description of the object of the contract would include description of a type of cloud computing services (**SaaS, PaaS, IaaS** or combination thereof), their **deployment model** (**public,** community**, private** or **hybrid**) and their technical, quality and performance characteristics and any applicable standards. Several documents comprising the contract may be relevant for determining the object of the contract [cross-link].

- *Service level agreement (SLA)*

43. The **SLA** contains **performance parameters** against which the delivery of the cloud computing services by the provider will be measured. It is thus an important

tool for determining the extent of the contractual obligations and possible contractual breaches of the provider. Standard provider **SLAs** may lack any specific obligations of result and instead contain non-enforceable statements of intent (e.g., "the provider will make best [or reasonable] efforts to ensure high service availability," "the provider will strive to keep services available 24 hours 7 days a week [or reach 99% uptime] (but does not guarantee that)"). The customer may lack any remedy under those contracts since the breach of professional best efforts provisions may be difficult to determine. To avoid such situations, the customer would be interested in including in the **SLA** quantitative and qualitative performance parameters with specific metrics, quality assurances and performance measurement methodology.

Examples of quantitative performance parameters

Capacity	- X capacity of data storage - X amount of memory available to the running program
Availability	- the amount or percentage of **uptime** (e.g., 99.9 per cent) - a detailed formula for calculation of **uptime** - specific dates or days and time when availability of the service is critical (100 per cent) - availability of a particular application (100 per cent)
Downtime or outages	- 10 outages of 6 minutes - 1 outage of 1 hour - time for restoring the data following a service outage
Elasticity and scalability	- how much and how fast services can be scaled up or down, e.g., maximum available resources within a minimum period
Latency	- less than X milliseconds
Encryption	- X bit value at rest, in transit and use
Support services	- 24/7 - typical operating hours of the customer
Incident and disaster management and recovery plans	- the maximum incident resolution time - the maximum **first response time** - **recovery point objectives (RPOs)** - **recovery time objectives (RTO)** - specific dates or days and time when it is critical to achieve recovery within X time frame
Persistency of data storage	- intact data /(intact data + lost data during X period of time (e.g., a calendar month)). The type of data (e.g., files, databases, codes, applications) and the unit of measurement (the number of files, bit length) would need to be defined.

Examples of qualitative performance parameters

Data portability	- the customer data is retrievable by the customer via a single download link or documented API

	- the data format is structured and documented in a sufficient manner to allow the customer to re-use it or to restructure it into a different data format if desired
Data localization requirements	- customer data (including any copy, **metadata**, and backup thereof) is stored exclusively in data centres physically located in the jurisdictions indicated in the contract and owned and operated by entities established in those jurisdictions — data is never to be moved outside country X, must be duplicated in country Y and elsewhere but never in country Z
Security	- the services provided under the contract are certified at least annually by an independent auditor against a security standard identified in the contract
Encryption	- the provider will ensure that customer data will be encrypted whenever it is transported over a public communication network, such as the Internet, both between the customer and the provider and between data centres used by the provider and whenever it is at rest in data centres used by the provider - the provider has implemented a key management policy in compliance with an international standard identified in the contract
Data protection/privacy	- the services provided under the contract are certified at least annually by an independent auditor against the data protection/privacy standard identified in the contract
Data deletion	- the provider ensures that the customer data is effectively, irrevocably and permanently deleted wherever requested by the customer within a certain time frame identified in the contract and in compliance with the standard or technique identified in the contract

44. The contract may need to include mechanisms to facilitate implementation of changes in the customer's demands. Otherwise, a potentially time consuming negotiation process may occur each time the customer's demands change.

Performance measurement

45. The contract may need to provide for the chosen measurement methodology and procedures, specifying in particular a reference period for measurement of services (daily, weekly, monthly), service delivery reporting mechanisms (frequency and form), role and responsibilities of the parties and the point of measurement. The parties may agree on independent measurement of performance and allocation of related costs.

46. The customer would be interested in measuring services during peak hours, i.e., when they are most needed. It may be in a position to measure, or verify the

measurements provided by the provider or third parties, of only those metrics that are based on performance at the point of consumption, but not those that are based on system performance at the point of provision of services. The customer may be in a position to evaluate the latter from reports provided by the provider or third parties. The provider may agree to provide the customer with performance reports on demand, periodically (daily, weekly, monthly, etc.) or following a particular incident. Alternatively, it may agree to grant the right to the customer to review the provider's records related to the service level measurements. Some providers enable customers to check data on service performance in real time.

47. The contract may oblige either or both parties to maintain records about the provision and consumption of services for a certain length of time. Such information may be useful in negotiating any amendments to the contract and in case of disputes.

- *Acceptable use policy (AUP)*

48. The **AUP** sets out conditions for use by the customer and its end-users of the cloud computing services covered by the contract. It aims at protecting the provider from liability arising out of the conduct of their customers and customers' end-users. Any potential customer is expected to accept such policy, and it will form part of the contract with the provider. The vast majority of standard AUPs prohibit a consistent set of activities that providers consider to be improper or illegal uses of **cloud computing services**. In some cases, removing some prohibitions may be justified in the light of specific needs of the customer.

49. It is usual for provider's standards terms to require that customer's end-users also comply with the **AUP** and to oblige the customer to use its best efforts or commercially reasonable efforts to ensure such compliance. Some providers may require customers to affirmatively prevent any unauthorized or inappropriate use by third parties of the cloud computing services offered under the contract. The customer may prefer to limit its obligations to communication of the **AUP** to known end-users and not to authorize or knowingly allow such uses, in addition to notifying the provider of all unauthorized or inappropriate uses of which it becomes aware.

- *Security policy*

50. Security of the system, including customer data security, involves shared responsibilities of the provider and the customer. The contract would need to specify reciprocal roles and responsibilities of the parties as regards security measures, reflecting obligations that may be imposed by mandatory law on either or both parties.

51. It is usual for the provider to follow its security policies. In some cases, it might be possible, although not in **standardized commoditized multi-subscriber solutions**, to negotiate that the provider will follow the customer's security policies. The contract may specify security measures (e.g., requirements for sanitization or deletion of data in the damaged media, the storage of separate packages of data in different locations, the storage of the customer's data on specified hardware that is unique to the customer). The parties would however need to assess risks of excessive disclosure of security information in the contract.

52. Some security measures would not presuppose the other party's input and would rely exclusively on the relevant party's routine activities, such as inspections by the provider of the hardware on which the data is stored and on which the services run and effective measures to ensure controlled access thereto. In other cases, allowing the party to perform its corresponding duties or evaluate and monitor the quality of security measures delivered may presuppose the input of the other party. The customer, for example, would be expected to update lists of users' credentials and their access rights and inform the provider of changes in time to ensure the proper identity and access management mechanisms. The customer would also be expected to identify to the provider the level of security to be allocated to each category of data.

53. Some threats to security may be outside the contractual framework between the customer and the provider and may require alignment of the terms of the cloud

computing contract with other contracts of the provider and the customer (e.g., with Internet service providers).

- *Data integrity*

54. Providers' standard contracts may contain a general disclaimer that ultimate responsibility for preserving integrity of the customer's data lies with the customer. Providers may offer only non-binding assurances that they will make best efforts to safeguard customer data.

55. Some providers may be willing to undertake data integrity commitments (for example, regular backups), possibly for additional payment. Regardless of the contractual arrangements with the provider, the customer may wish to consider whether it is necessary to secure access to at least one usable copy of its data outside of the provider's and its sub-contractors' control, reach or influence and independently of their participation.

- *Confidentiality clause*

56. In some cases, the provider does not offer a confidentiality or non-disclosure clause or these clauses are not sufficient to guarantee respect for confidentiality of customer data. Some providers may even expressly waive any duty of confidentiality regarding customer data, shifting full responsibility for keeping data confidential to the customer, e.g., through encryption. Providers may only agree to assume liability for confidentiality of data disclosed by the customer during contract negotiations, but not for data processed during service provision. The provider's willingness to commit to ensuring confidentiality of customer data would depend on the nature of services provided to the customer under the contract, in particular whether the provider will be required to have unencrypted access to data for the provision of those services.

57. In most cases, the customer will want the provider to ensure confidentiality for all customer data placed in the cloud and undertake a higher level of confidentiality commitments as regards some sensitive data (with a separate liability regime for breach of confidentiality of such data). The customer may in particular be concerned about its trade secrets, know-how and information that it is required to keep confidential under law or commitments to third parties.

58. Where an extra layer of protection is necessary, it may be appropriate to restrict access to the customer data to a limited set of the provider's personnel and to require the provider to obtain individual confidentiality commitments from them, in particular from those with high-risks roles (e.g., system administrators, auditors and persons dealing with intrusion detection reports and incident response). It would be for the customer to properly specify to the provider the confidential information, the required level of protection, any applicable law or contractual requirements and any changes affecting such information, including any changes in the applicable legislation.

59. In some cases, the disclosure of customer data may be necessary for fulfilment of the contract. In other cases, the disclosure may be mandated by law, for example, under the duty to provide information to competent State authorities [cross-link]. Appropriate exceptions to confidentiality clauses would thus be warranted.

60. The provider may in turn wish to impose on the customer the obligation not to disclose information about the provider's security arrangements and other details of services provided to the customer under the contract or law.

- *Data protection/privacy policy or data processing agreement*

61. **Personal data** is subject to special protection by law in many jurisdictions. Law applicable to the **processing** of such data may be different from the law applicable to the contract and will override any non-compliant contractual clauses.

62. The contract may include a data protection or privacy clause, data processing agreement or similar type of agreement, although some providers may only agree to the general obligation to comply with applicable data protection laws. In some

jurisdictions, such general commitment may be insufficient: the contract would need to stipulate at a minimum the subject-matter, duration, the nature and purpose of the **processing**, the type of **personal data** and categories of **data subjects** and the obligations and rights of the **data controller** and the **data processor**. Where the possibility of negotiating a data protection clause in the contract does not exist, the customer may need at least to review standard terms to determine whether the provisions give the customer sufficient guarantees of lawful **personal data processing** and adequate remedies for damages.

63. The customer will likely be **data controller** and will assume responsibility for compliance with data protection law in respect of **personal data** collected and processed in the cloud. The customer may need to seek contractual clauses that would oblige the provider to support the customer's compliance with the applicable data protection regulations, including requests related to **data subjects' rights**. Separate remedies could be negotiated should the provider breach that obligation, including the possibility of unilateral termination of the contract by the customer and provider compensation for damages.

64. Providers' standard contracts usually stipulate that the provider does not assume any **data controller** role. The provider will likely act only as **data processor** when it processes the customer data according to instructions of the customer for the sole purpose of providing the cloud computing services. The provider may however be regarded as **data controller,** regardless of contractual clauses, when it further processes data for its own purposes or upon instructions of State authorities [cross-link]. It would assume full responsibility for **personal data** protection in respect of that further **processing**.

- *Obligations arising from data breaches and other security incidents*

65. The parties may be required under law or contract or both to notify each other immediately of a security incident of relevance to the contract or any suspicion thereof that becomes known to them. That obligation may be in addition to general notification of a security incident that may be required under law to inform all relevant stakeholders, including **data subjects**, insurers and State authorities, in order to prevent or minimize the impact of security incidents.

66. The parties may agree on the notification period (e.g., one day after the party becomes aware of the incident or threat), form and content of the **security incident notification** and **post-incident steps**, which may vary depending on the categories of data stored in the cloud. Any notification requirements should recognize the need not to disclose any sensitive information that could lead to the compromise of the affected party's system, operations or network.

67. The customer may wish to reserve the right to terminate the contract in case of a serious security incident resulting, for example, in loss of customer data.

D. Rights to customer data and other content

- *Provider rights to customer data for the provision of services*

68. Providers usually reserve the right to access customer data on the "need-to-know" principle. That arrangement would allow access to customer data by the provider's employees, sub-contractors and other third parties (e.g., auditors) where necessary for the provision of the cloud computing services (including maintenance, support and security purposes) and for monitoring compliance with applicable **AUP, SLA**, **IP licences** and other contractual documents. Customers may be interested to narrow down circumstances when access would be allowed and insist on measures that would ensure confidentiality and integrity of customer data.

69. Certain rights to access customer data can be considered to be implicitly granted by the customer to the provider by requiring a certain service or feature: without those rights, the provider will not be able to perform the services. For example, if the

provider is required to regularly backup customer data, the fulfilment of that task necessitates the right to copy the data. Likewise, if sub-contractors are to handle customer data, the provider must be able to transfer the data to them.

70. The contract may explicitly indicate which rights concerning data required for the performance of the contract the customer grants to the provider, whether and to what extent the provider is entitled to transfer those rights to third parties (e.g., to its sub-contractors) and the geographical and temporal extent of the granted or implied rights. The geographical limitations could be particularly important for the customer if it wishes to prevent data from leaving a certain country or region. The contract would also typically state whether the customer would be able to revoke granted or implied rights and under what conditions. Since the ability to provide the services at the required level of quality may depend on the rights granted by the customer, the direct impact of revocation of certain rights could be the amendment or termination of the contract.

- *Provider use of customer data for other purposes*

71. The provider may request use of customer data for purposes other than those linked to the provision of the cloud computing services under the contract (e.g., for advertising, generating statistics, analytical or predictions reports, engaging in other data mining practice). The questions for the customer to consider in that context include: (a) which information about the customer and its end-users will be collected and the reasons for and purposes of its collection and use by the provider; (b) whether that information will be shared with other organizations, companies or individuals and if so, the reasons for doing so and whether this will be done with or without the customer's consent; and (c) how compliance with confidentiality and security policies will be ensured if the provider shares that information with third parties. Where the provider's use of customer data will affect **personal data**, the parties would need in addition to carefully assess their regulatory compliance obligations under applicable data protection laws.

72. Generally, the contract may need to state that the provider acquires no automatic rights to use the customer data for its own purposes. The contract can list permissible grounds for the use of the customer data other than for the purposes of the provision of the services. For example, the contract could permit the provider to use data as anonymized open data or in aggregated and de-identified form for its own purposes during the term of the contract or beyond. In such cases, the contract may include obligations regarding de-identification and anonymization of customer data to ensure compliance with any applicable data protection and other regulations. It may also impose limits on reproduction of content and communication to public.

- *Provider use of customer name, logo and trademark*

73. Providers' standard terms may grant the provider the right to use customer names, logos and trademarks for purposes of the provider's publicity. The customer may negotiate deletion or modification of such provisions. For example, it may require the provider to seek prior approval by the customer of the use of its name, logo and trademark or it may limit the permissible use to the customer name.

- *Provider actions as regards customer data upon State orders or for regulatory compliance*

74. Provider' standard terms may reserve a provider's broad discretion to disclose, or provide access to, customer data to State authorities (e.g., by including such wording as "when doing so will be in the best interests of the provider"). The customer may be interested to narrow down circumstances in which the provider will be able to do so, for example when the provider faces an order from a court or other State authority to provide access to data or to delete or change it (e.g., enforcing **data subjects' right** to be forgotten). The provider may however insist on its right to remove or block customer data immediately in other cases, irrespective of State orders, e.g., after the provider gains knowledge or becomes aware of illegal content, to avoid liability under law (the "notice and takedown" procedure [cross-link]).

75. At a minimum, the contract may oblige the provider to notify the customer immediately of State orders or the provider's own decisions as regards customer data with a description of the data concerned, unless such notification would violate law. Where the advance notification and involvement of the customer is not possible, the contract may require the provider to serve immediate ex-post notification to the customer of the same information. The contract may oblige the provider to keep, and provide customer access to, logs of all orders, requests and other activities as regards customer data.

- *Rights to cloud service derived data*

76. The contract may need to address customer rights to **cloud service derived data** and how such rights can be exercised during the contractual relationship and upon termination of the contract.

- *IP rights protection clause*

77. Some types of cloud computing contracts may result in the creation of objects of IP rights, either jointly by the provider and the customer (e.g., service improvements arising from the customer's suggestions) or by the customer alone (new applications, software and other original work). The contract may contain an express IP clause that will determine which party to the contract owns IP rights to various objects deployed or developed in the cloud and the use that the parties can make of such rights. Where no option to negotiate exists, the customer may need at least to review any IP clauses to determine whether the provider offers sufficient guarantees and allows the customer appropriate tools to protect and enjoy its IP rights and avoid **lock-in** risks [cross-link].

- *Data retrieval for legal purposes*

78. Customers may be required to be able to search and find data placed in the cloud in its original form for legal purposes, such as in legal proceedings. The electronic records may in particular be required to be capable meeting auditing and investigation standards. Some providers may be in a position to offer assistance to customers with the retrieval of data in the format required by law for legal purposes. In such cases, the contract may need to define exactly the assistance the customer would require from the provider to fulfil requests of competent authorities for data retrieval for legal purposes.

- *Data deletion*

79. Data deletion considerations will be applicable during the term of the contract, but particularly upon its termination. For example, certain data may need to be deleted according to the customer's retention plan. Sensitive data may need to be destroyed at a specified time in its lifecycle (e.g., by destruction of hard disks at the end of the life of equipment that stored such data). Data may also need to be deleted in order to comply with law enforcement deletion requests or after confirmed IP infringement cases [cross-link].

80. Provider' standard terms may contain only non-binding statements to delete customer data from time to time. The customer may be interested to oblige the provider to delete data, its backups and **metadata** immediately, effectively, irrevocably and permanently, in compliance with the data retention and disposition schedules or other form of authorization or request communicated by the customer to the provider. The contract may address the time period and other conditions for data deletion, including the provider's obligation to serve the customer with a confirmation of the data deletion upon completion of the deletion and to provide customer access to audit trails of the deletion activities.

81. Particular standards or techniques for deletion may be specified, depending on the nature and sensitivity of the data (e.g., deletion may be required from different locations and media, including from sub-contractors' and other third parties' systems, with different levels of deletion, such as data sanitization ensuring confidentiality of the data until its complete deletion or hardware destruction). More secure deletion

involving destruction rather than redeployment of equipment may be more expensive and not always possible (if for example data of the provider's other customers is stored on the same hardware). Those aspects would need to be taken into account in negotiating the contract, for example by requiring the provider to use an isolated infrastructure for storing a customer's particularly sensitive data.

E. Audits and monitoring

- *Monitoring activities*

82. The parties may need to monitor activities of each other to ensure regulatory and contractual compliance (e.g., compliance of the customer and its end-users with **AUP** and **IP licenses** and compliance of the provider with **SLA**, data protection policy, etc.). Some monitoring activities, such as those related to **personal data processing,** may be mandated by law.

83. The contract should identify periodic or recurrent monitoring activities together with the party responsible for their performance and obligations of the other party to facilitate monitoring. The contract may also anticipate any exceptional monitoring activities and provide options for handling them. The contract may also provide for reporting requirements to the other party as well as any confidential undertakings in conjunction with such monitoring activities.

84. Excessive monitoring may affect performance and increase costs of services. For services requiring near real-time performance, the customer may wish to seek the right to require the provider to pause or stop monitoring if it is materially detrimental to the service performance.

- *Audit and security tests*

85. Audit and security tests, in particular initiated by the provider to check the effectiveness of security measures, are common. Some audits and security tests may be mandated by law. The contract may include clauses that would address the audit rights of both parties, the scope of audits, recurrence, formalities and costs. It may also oblige the parties to share with each other the results of the audits or security tests that they commission. The contractual rights or statutory obligations for audit and security tests may need to be complemented in the contract with corresponding obligations of the other party to facilitate the exercise of such rights or fulfilment of those obligations (e.g., to grant access to the relevant data centres).

86. Parties may agree that audits or security tests may only be performed by professional organizations or that the provider or the customer may choose to have the audit or security test performed by a professional organization. The contract may specify qualifications to be met by the third party and conditions for their engagement, including allocation of costs. Special arrangements may be agreed upon by the parties for audits or security tests subsequent to an incident and depending on the severity and type of the incident (for example, the party responsible for the incident may be obliged to partially or fully reimburse costs).

F. Payment terms

- *Pay-as-you-go*

87. Price is an essential contractual term, and failure to set the price or a mechanism for determining the price may render the contract unenforceable.

88. The **on-demand self-service** characteristic of cloud computing is usually reflected in the **pay-as-you-go** billing system. It is common for the contract to specify the price per unit for the agreed volume of supply of the cloud computing services (e.g., for a specified number of users, number of uses or time used). Price scales or other price adjustments, including volume discounts, may be designed as incentives or penalties for either of the parties. Free trials are common as is not charging for

some services. Although there could be many variations for price calculation, a clear and transparent price clause, understood by both parties, may avoid future conflict and litigation.

- *Licensing fees*

89. The contract should make it clear whether the payment for the cloud computing services encompasses licensing fees for any licences the provider may grant to the customer as part of the services. **SaaS**, in particular, often involve the use by the customer of software licensed by the provider.

90. The licensing fees may be calculated on a per-seat or per instance basis and fees may vary depending on the category of users (e.g., professional users, as opposed to non-professional users, may be in one of the most expensive categories). The customer would need to consider the implications of various payment structures. For example, a customer's licence costs may increase exponentially if software is charged on a per instance basis each time a new machine is connected, even though the customer is using the same number of machine instances for the same duration. It would also be important for the customer to identify in the contract not only the number of potential users of a software covered by the licence arrangement, but also the number of users in each category (for example, employees, independent contractors, suppliers) and rights to be granted to each category of users. The customer would also want the contract to identify access and use rights that will be included in the scope of the licence and cases of access and use by the customer and its end-users that may lead to an expanded scope of the license and consequently increased licensing fees.

- *Additional costs*

91. The price may cover also one-off costs (e.g., configuration and migration to the cloud). There could also be additional services not included in the basic cloud computing service contract but offered by the cloud computing service provider against separate payment (e.g., support after business hours charged per time or provided for a fixed price). The parties should also clarify the impact of taxes since cloud computing services may or may not fall within the category of taxable services or goods.

- *Changes in price*

92. Providers' standard terms often give the provider the right to unilaterally modify the price or price scales. The customer may prefer to limit that right. The parties may agree to specify in the contract the pricing methodology (e.g., how frequently the provider can increase prices and by how much). The prices may be capped to a specific consumer price index, to a set percentage or to the provider's list price at a given moment. The customer may require the provider to serve advance notice of a price increase and stipulate in the contract the consequences of non-acceptance of the price increase by the customer.

- *Other payment terms*

93. Payment terms may need to cover invoicing modalities (e.g., e-invoicing) and the form and content of the invoice, which may be important for tax regulations compliance. Tax authorities of some jurisdictions may not accept electronic invoices or may require a special format, including that any tax applicable to the cloud computing services may need to be stated separately.

94. The contract may also need to specify payment due date, currency, the applicable exchange rate, manner of payment, sanctions in case of late payment and procedures for resolving disputes over payment claims.

G. Changes in services

95. **Cloud computing services** by nature are flexible and fluctuating. The contract may contain many options the customer may use to adjust services to its evolving business needs. In addition, the provider may reserve the right to adjust its service portfolio at its discretion. Different contractual regimes may be appropriate depending on whether changes concern the core services or ancillary services and support aspects. Different contractual regimes may also be justified for changes that might negatively affect services as opposed to service improvements (e.g., a switch from a standard offering to an enhanced cloud computing offering with higher security levels or shorter response times).

- *Upgrades*

96. Although upgrades may be in the customer's interests, they may also cause disruptions in the availability of cloud computing services since they could translate into relatively high **downtime** during normal working hours even if the service is to be provided on 24/7 basis. They may also have other negative impact, for example requiring changes to customer applications or IT systems or calling for retraining of customer users.

97. The contract may require the provider to notify the customer well in advance of pending upgrades and implications thereof. The provider may be obliged to schedule upgrades during period of little or no demand for the customer. The parties may agree that the older version should be retained in parallel with the new version for an agreed period of time where significant changes are made to the previous version, to ensure the customer business continuity. Procedures for reporting and solving possible problems may need to be agreed. The contract may also need to address assistance to be provided by the provider with changes to customer applications or IT systems and with retraining of the customer's end-users when required. The parties may also need to agree on allocation of costs arising from upgrades.

- *Degradation or discontinuation of services*

98. Technological developments, competitive pressure or other reasons may lead to degradation of some cloud computing services or their discontinuation with or without their replacement by other services. The provider may reserve in the contract the right to adjust the service portfolio offering, e.g., by terminating a portion of the services. Discontinuation of even some cloud computing services by the provider may however expose the customer to liability to its end-users.

99. The contract may need to build in adequate protection for the customer in such cases, including an advance notification of those changes to the customer, the customer right to terminate the contract in the case of unacceptable changes and an adequate retention period to ensure the timely **reversibility** of any affected customer data or other content. The contract may altogether prohibit modifications that could negatively affect the nature, scope or quality of provided services, or limit the provider's right to introduce only "commercially reasonable modifications". The customer would however not necessarily be always in the best position to judge on reasonableness of modifications to the services provided and might need to rely in that respect on advice of independent experts.

- *Suspension of services at the provider's discretion*

100. Providers' standard terms may contain the right of the provider to suspend services at its discretion at any time. The customer may wish to restrict such unconditional right by not permitting suspension except for clearly limited cases (e.g., in case of the fundamental breach of the contract by the customer, for example non-payment). "Unforeseeable events" is a common justification for unilateral suspension of services by the provider. Such events are usually defined broadly encompassing any impediments beyond the provider's control, including failures of sub-contractors, sub-providers and other third parties involved in the provision of the cloud computing services to the customer, such as Internet network providers.

101. The customer may consider conditioning the right of suspension due to unforeseeable events on the provider properly implementing a business continuity and disaster recovery plan. The contract may require that such plan contain protections against common threats to the provision of the cloud computing services and be submitted for comment and approval by the customer. Those protections may include a geographically separate disaster recovery site with seamless transition and the use of an uninterruptible power supply and back-up generators.

- *Notification of changes*

102. Providers' standard terms may contain no obligation on the provider to notify the customer regarding changes in the terms of services. Customers may be required to check regularly whether there have in fact been any changes in contractual documents hosted on the provider's website(s). Those contractual documents may be numerous; some may incorporate by reference terms and policies contained in other documents, which may in turn incorporate by reference additional terms and policies, all of which may be subject to unilateral modification by the provider. It might therefore not be easy for the customer to notice changes introduced by the provider.

103. Since the continued use of services by the customer is deemed to be acceptance of the modified terms, the customer may wish to include in the contract an obligation for the provider to notify the customer of changes in the terms of services sufficiently in advance of their effective date. The contract may also oblige the provider to give the customer access to audit trails concerning evolution of services. The customer may also wish to preserve all agreed terms and oblige the provider to define the services by reference to a particular version or release.

H. Sub-contractors, sub-providers and outsourcing

- *Identification of the sub-contracting chain*

104. Sub-contracting, **layered cloud computing services** and outsourcing are common in **cloud computing.** Providers' standard terms may explicitly reserve the provider's right to use third parties for provision of the cloud computing services to the customer or that right may be implicit because of the nature of services to be provided. The provider may be interested in retaining as much flexibility as possible in that respect.

105. Identifying in the contract third parties involved in the provision of the cloud computing services to the customer may be required by law or be beneficial to the customer for verification purposes. The customer would in particular be interested in seeking assurances concerning compliance of third parties with security, confidentiality, data protection and other requirements arising from the contract or law, the absence of conflicts of interest and the risks of non-performance of the contract by the provider due to failures of third parties. Although the provider may not be always in a position to identify all third parties involved in the provision of the cloud computing services to the customer, it should be able to identify those playing key roles.

- *Changes in the sub-contracting chain*

106. The contract may prohibit further changes in the sub-contracting chain without the customer's consent. It may provide for the customer's right to vet and veto any new third party involved in the provision of the cloud computing services to the customer. Alternatively, the contract may include the list of third parties pre-approved by the customer from which the provider can choose when the need arises.

107. The provider may however insist on its right to make unilateral changes in its sub-contracting chain with or without notification of the customer. The customer may wish to reserve the right to allow the provider to implement the change subject to subsequent approval by the customer. In the absence of such approval, it might be agreed that services would need to continue with the previous or other pre-approved

third party or with another third party to be agreed by the parties; otherwise, the contract may be terminated. Mandatory applicable law may stipulate circumstances in which changes in a provider's sub-contracting chain may require termination of the contract.

- *Alignment of contract terms with linked contracts*

108. Although third parties instrumental to the performance of the cloud computing contract may be listed in the contract, they would not be parties to the contract between the provider and the customer. They would be liable for obligations under their contracts with the provider. Nevertheless, various mechanisms may exist to ensure that the terms of the contract between the customer and the provider are made binding on those third parties. In particular, the contract may require the provider to align the terms of the contract with existing or future linked contracts. The contract may also require the provider to supply the customer with copies of linked contracts for verification purposes.

109. The customer may opt to contract with third parties instrumental to the performance of the cloud computing contract directly, in particular on such sensitive issues as confidentiality and **personal data processing**. It may also want to negotiate with key third parties obligations to step in if the provider fails to perform under the contract, including in case of the provider's insolvency.

- *Liability of sub-contractors, sub-providers and other third parties*

110. Under applicable law or contract, the provider may be held liable to the customer for any issue within the responsibility of any third party whom the provider involved in the performance of the contract. In particular, the joint liability of the provider and its sub-contractors may be established by law for any issues arising from **personal data processing**, depending on the extent of sub-contractors' involvement in processing.

111. The contract could oblige the provider to create third party beneficiary rights for the benefit of the customer in linked contracts or make the customer a party to linked contracts. Both options would allow the customer to have direct recourse against the third party in case of its non-performance under a linked contract.

I. Liability

- *Allocation of risks and liabilities*

112. In business to business transactions, the parties are free to allocate risks and liabilities as they consider appropriate, subject to any mandatory provisions of applicable law. Factors such as risks involved in the provision of the cloud computing services, whether they are provided for remuneration or otherwise and the amount charged for the cloud computing services by the provider would all be considered in negotiating the allocation of risks and liabilities. Although parties generally tend to exclude or limit liability as regards factors that they cannot control or can control only to a limited extent (e.g., behaviour of end-users, actions or omissions of sub-contractors), the level of control would not always be a decisive consideration. A party may be prepared to assume risks and liability for elements that it does not control in order to distinguish itself in the market place. It is nevertheless likely that the party's risks and liabilities would increase progressively in proportion to the components under its control.

113. For example, in **SaaS** involving the use of standard office software, it is likely that the provider would be responsible for virtually all resources provided to the customer, and liability of the provider could arise in each case of non-provision or malfunctioning of those resources. Nevertheless, even in those cases, the customer could still be responsible for some components of the services, such as encryption or backups of data under its control. The failure to ensure adequate backups might lead to the loss of the right of recourse against the provider in case of the loss of data. On

the other hand, in **IaaS** and **PaaS**, the provider could be responsible only for the infrastructure or platforms provided (such as hardware resources, operating system or middleware), while the customer would assume responsibility for all components belonging to it, such as applications run using the provided infrastructure or platforms and data contained therein.

- *Exclusion or limitation of liability*

114. Providers' standard terms may exclude any liability under the contract and take the position that liability clauses are non-negotiable. Alternatively, the provider may be willing to accept liability, including unlimited liability, for breaches controllable by the provider (e.g., a breach of IP licenses granted to the provider by the customer) but not for breaches that may occur for reasons beyond the provider's control (e.g., security incidents, unforeseeable events or leaks of confidential data). Providers' standard terms generally exclude liability for indirect or consequential loss (e.g., loss of business opportunities following the unavailability of the cloud computing service).

115. Where liability is accepted generally or for certain specified cases, providers' standard terms often limit the amount of losses that will be covered (per incident, per series of incidents or per period of time). In addition, providers often fix an overall cap on liability under the contract, which may be linked to the revenue expected to be received under the contract, to the turnover of the provider or insurance coverage.

116. The customer may be interested in negotiating unlimited liability or higher compensation for defined types of damage caused by an act or omission of the provider or its personnel. The ability to do so may depend, among other factors, on the **deployment model** [cross-link]. Customer data loss or misuse, personal data protection violations and IP rights infringement in particular could lead to potentially high liability of the customer to third parties or give rise to regulatory fines. Imposing a more stringent liability regime on the provider where those cases are due to the provider's fault or negligence may be justified. Unlimited liability of the provider may also flow from certain types of defects under law (e.g., defective hardware or software).

117. Providers' standard terms usually impose liability on the customer for non-compliance with **AUP**. The customer may wish to limit its liability arising from violation of **AUP** in particular for actions of its end-users that it cannot control.

118. Disclaimers and limitations of liability may need to be contained in the main body of the contract and properly communicated to the other party in order to be enforceable.

- *Liability insurance*

119. The contract may contain insurance obligations for both or either party, in particular as regards quality requirements for an insurance company and the minimum amount of insurance coverage sought. It may also require parties to notify changes to the insurance coverage or provide copies of current insurance policies to each other.

- *Statutory requirements*

120. While most legal systems generally recognize the right of contracting parties to allocate risks and liabilities and limit or exclude liability through contractual provisions, this right is usually subject to various limitations and conditions. For example, an important factor in risk and liability allocation in **personal data processing** is the role that each party assumes as regards the **personal data** placed in the cloud. The data protection law of many jurisdictions imposes more liability on the **data controller** than on **data processors** of **personal data**. Notwithstanding contractual provisions, the factual handling of such data will generally determine the legal regime to which the party would be subject under the applicable law. **Data subjects** who have suffered loss resulting from an unlawful processing of **personal data** or any act incompatible with domestic data protection regulations may be entitled to compensation directly from the **data controller**.

121. In addition, in many jurisdictions, a total exclusion of liability for a person's own fault is not admissible or is subject to limitations. It might not be possible to exclude altogether liability related to personal injury (including sickness and death) and for gross negligence, intentional harm, defects, breach of core obligations essential for the contract or non-compliance with applicable regulatory requirements. Moreover, if the terms of the contract are not freely negotiated, but rather are imposed or pre-established by one of the parties ("contracts of adhesion"), some types of limitation clauses may be found to be "abusive" and therefore invalid [cross-link].

122. The ability of public institutions to assume certain liabilities may be restricted by law, or public institutions would need to seek prior approval of a competent State body for doing so. They may also be prohibited from accepting exclusion or limitation of a provider's liability altogether or for acts or omissions defined in law.

123. The applicable law may, on the other hand, provide for exemption from liability if certain criteria are fulfilled by a party that would otherwise face a risk of liability. For example, under the "notice and take down" procedure in some jurisdictions, the provider will be released from liability for hosting the illegal content on its cloud infrastructure if it removed such content once it became aware of it [cross-link].

J. Remedies for breach of the contract

- *Types of remedies*

124. Within the limits provided by applicable law, the parties are free to select remedies. Remedies may include in-kind remedies aimed at providing the aggrieved party with the same or equivalent benefit expected from contract performance (e.g., replacement of the defective hardware), monetary remedies (e.g., service credits) and termination of the contract. The contract could differentiate between types of breaches and specify corresponding remedies.

- *Suspension or termination of services*

125. Suspension or termination of the provision of the cloud computing services to the customer is a usual remedy of the provider for the customer's breach of a contract or violation of **AUP** by the customer's end-users. The customer would be interested in contractual safeguards against broad suspension or termination rights. For example, the right of the provider to suspend or terminate the provision of the cloud computing services to the customer may be limited to cases of fundamental breach of the contract by the customer and significant threats to the security or integrity of the provider's system. The provider's right to suspend or terminate may also be restricted only to those services that are affected by the breach, where such a possibility exists.

- *Service credits*

126. An often-used mechanism to compensate the customer for non-performance by the provider is the system of service credits. These credits take the form of a reduced fee for the services to be provided under the contract in the following measured period. A sliding scale may apply, i.e., a percentage of reduction may depend on the extent to which the provider's performance under the contract falls short of the performance parameters identified in **SLA** or other parts of the contract. An overall cap for service credits may also apply. Providers may limit the circumstances in which service credits are given to those, for example, where failures arise from matters under the provider's control or where credits are claimed within a certain period of time. Some providers may also be willing to offer a refund of fees already paid or an enhanced service package in the following measured period (e.g., free IT consultancy). If a range of options exists, providers' standard terms usually stipulate that any remedy for provider non-performance will be at the choice of the provider.

127. The customer would need to assess on a case-by-case basis the appropriateness of the contract fixing service credits as the sole and exclusive remedy against the provider's non-performance of its contractual commitments. Doing so may limit the

customer's rights to other remedies, including suing for damages or terminating the contract. The customer may be interested in the contract providing other measures to mitigate risks of non-performance by the provider, as well as sufficient incentives for the provider to perform well under the contract and improve services. Penalties for example could have a bigger financial impact on the provider than service credits. In addition, service credits in the form of fee reduction or an enhanced service package in the following measured period may be useless if the contract is to be terminated. Excessive service credits may be unenforceable if they have been considered as an unreasonable approximation of harm at the outset of the contract.

- *Formalities to be followed in case of the breach of the contract*

128. The contract may include formalities to be followed in cases of breach. For example, the contract could require a party to notify the other party when any terms of the contract are deemed to be violated and to provide a chance to remedy such asserted violation. Time limits for claiming remedies may also be set.

K. Term and termination of the contract

- *Effective start date of the contract*

129. The effective start date of the contract would need to be clearly stated in the contract. It may be different from the signature date, the date of acceptance of the offer or the date of acceptance of configuration and other actions required for the customer to migrate to the cloud. The date when the cloud computing services are made available to the customer by the provider, even if they are not actually used by the customer, may be considered the effective start date of the contract. The date of the first payment by the customer for the cloud computing services, even if they are not yet made available to the customer by the provider, may also be considered the effective start date of the contract.

- *Duration of the contract*

130. The duration of the contract could be short, medium or long. It is common in **standardized commoditized multi-subscriber cloud solutions** to provide for a fixed initial duration (short or medium), with automatic renewals unless terminated by either party. The customer may oblige the provider to notify the customer of the upcoming expiration of the term of the contract and the need to take a decision about renewal. That mechanism may be useful for the customer in efforts to avoid risks of **lock-in** and missing better deals.

- *Earlier termination*

131. The contract would address circumstances in which the contract could be terminated other than upon expiration of its fixed term, such as for convenience, breach or other reasons. The contract may need to provide modalities for earlier termination, including requirements for a sufficiently advance notice, **reversibility** and other end-of-service commitments [cross-link].

Termination of the contract for convenience

132. Providers' standard terms, especially for provision of **standardized commoditized multi-subscriber cloud** solutions**,** usually reserve the right of the provider to terminate the contract at any time without customer default. The customer may wish to limit the circumstances under which such a right could be exercised and oblige the provider to serve the customer with sufficiently advance notice of termination.

133. The customer's right to terminate the contract for convenience (i.e., without the default of the provider) is especially common in public contracts. The provider may demand payment of early termination fees in such cases. Payment of early termination fees by public entities may however be restricted by law. In contracts of indefinite duration, providers may be more inclined to accept termination by the customer for

mere convenience without compensation, but that might also lead to a higher contract price.

Termination for breach

134. Fundamental breach of the contract usually justifies termination of the contract. To avoid ambiguities, the parties may define in the contract events that will be considered by the parties fundamental breach of the contract. For the customer, those may include data loss or misuse, personal data protection violations, recurrent security incidents (e.g., more than X times per any measured period), confidentiality leaks and non-availability of services at certain time points or for certain period of time. Non-payment by the customer and violation by the customer or its end-users of **AUP** are among the most common reasons for termination of the contract by the provider. The party's right to terminate the contract may be conditional on serving a prior notice, holding good faith consultations, providing a possibility to remedy the situation and committing to restoration of contract performance within a certain number of days after remedial action has been taken.

135. The contract may need to address the provider's end-of-service commitments that would survive the customer's fundamental breach of the contract. The customer would want to ensure, at a minimum, **reversibility** of its data and other content [cross-link].

Termination due to unacceptable modifications of the contract

136. Unacceptable, commercially unreasonable modifications or materially detrimental unilateral modifications to the contract may justify termination of the contract. Those modifications might include modifications to **data localization** requirements or sub-contracting terms. The contract may need specifically to preserve the customer's right to terminate the entire contract if modifications to the contract due to the restructuring of the provider's service portfolio lead to termination or replacement of some services [cross-link].

Termination in case of insolvency

137. An insolvent customer may need to continue using the cloud computing services while resolving its financial difficulty. The customer may thus be interested in restricting the right of the provider to invoke the insolvency of the customer as the sole ground for termination of the contract in the absence of, for example, the customer's default in payment under the contract.

138. Risks of insolvency of the provider may be identified during the risk assessment. The contract may require the provider to supply the customer with periodic reports about the provider's financial condition and provide for the customer's right to terminate the contract without further obligation or liability in event the provider lacks the financial ability to fully perform the contract.

139. Risks of never being able to retrieve data and other content from the insolvent provider's cloud infrastructure are high where a mass exit and withdrawal of content occurs due to a crisis of confidence in the provider's financial position. The insolvent provider or an **insolvency representative** may limit the amount of content (data and application code) that can be withdrawn in a given time frame. It may also be decided that end-of-service commitments should proceed on a first come first served basis. The customer may therefore be interested in contractual mechanisms to ensure that it will be able to retrieve its data from the insolvent provider. The customer could request source code or key escrow that would automatically be released and allow access to the customer data and other content upon the provider's insolvency. Mandatory provisions of insolvency law may however override contractual undertakings.

Termination in case of change of control

140. The change of control may for example involve a change in the ownership or the capacity to determine, directly or indirectly, the operating and financial policies of the provider, which may lead to changes in the provider's service portfolio. The change of control may also involve the assignment or novation of the contract, with rights and obligations or only rights under the contract transferred to a third party. As a result, an original party to the contract may change or certain aspects of the contract, for example payments, may need to be performed to a third party.

141. The contract may need to oblige the provider to serve an advance notice of an upcoming change of control and its expected impact on continuity of services. The customer may be interested in reserving its contractual right to terminate the contract if, as a result of the change of control, the provider or the contract is taken over by the customer's competitor or if the take-over leads to discontinuation of, or significant changes in, the service portfolio. The applicable law may require termination of the contract if as a result of the change of control, mandatory requirements of law (e.g., data localization requirements or prohibition to deal with certain entities under international sanctions regime or because of national security concerns) cannot be fulfilled. Public contracts may in particular be affected by statutory restrictions on the change of control.

Inactive account clause

142. Customer inactivity for a certain time period specified in the contract may be a ground for unilateral termination of the contract by the provider. The inactive account clause would however rarely, if at all, be found in business to business cloud computing contracts provided for remuneration.

L. End of service commitments

143. End of service commitments may raise not only contractual but also regulatory issues. The contract would need to achieve a balance between the customer's interest in continuous access to its data and other content, including during the transition period, and the provider's interest in ending any obligation towards the former customer as soon as possible.

144. End of service commitments may be the same regardless of the cause of termination of the contract or may be different depending on whether termination is for the breach of the contract or other reasons. Issues that may need to be addressed by the parties in the contract include:

- *Timeframe for export*

145. The customer would be interested in a sufficiently long period to ensure smooth transition by the customer of its data and other content to another provider or back in-house.

- *Customer access to the content subject to export*

146. The contract would need to specify data and other content subject to export and ways of gaining customer access thereto, including any decryption keys that may be held by the provider or third parties. The parties may agree on an escrow to ensure automatic access by the customer to all attributes required for export. The contract may also specify export options, including their formats and processes, to the extent possible, recognizing that they may change over time.

- *Export assistance by the provider*

147. The extent, procedure and time period for the cloud provider's involvement in export of the customer data to the customer or to another provider of the customer's choice may need to be specified in the contract. The provider may require separate payment for the provision of export assistance. In such case, the parties may fix the

amount of the payment in the contract or agree to refer to the provider's pricing list at a given time. Alternatively, the parties may agree that such assistance is included in the contract price or that no extra payment will be charged if the contract termination follows the provider's breach of the contract.

- *Deletion of data from the provider's cloud infrastructure*

148. The contract may need to specify rules for deletion of the customer data and other content from the provider's cloud infrastructure upon export or expiration of the period specified in the contract for export. The data can be deleted automatically by the provider or upon a specific customer's request and instructions. The contract can include an obligation for the provider to alert the customer before the data is deleted and to confirm to the customer the deletion of data, backups and **metadata**. The provider may be obliged to deliver an attestation, report or statement of deletion, including deletion from third parties' systems.

- *Post-contract retention of data*

149. The provider might be required to retain customer data by law, in particular data protection law, which might also address a time frame during which the data must be retained. In addition, the customer may allow the provider to retain specified data or may wish the provider to contractually commit on retention of data after the termination of the contract for regulatory, litigation and other legal reasons affecting the customer. Some providers may allow customers to choose a post-contract retention period at additional cost.

150. Special requirements (e.g., to de-identify personal information) may need to be set out as regards data that is not or cannot be returned to the customer and whose deletion would not be possible. The contract would need to specify the format in which that data is to be retained after termination of the contract. It may be a format approved by the customer (an encrypted or unencrypted format), or the contract may state generally that the data is to be retained in a usable and interoperable format to allow its retrieval when required. The contract would need to specify the responsibilities of the parties for post-contractual retention of the data in the specified format.

- *Post-contract confidentiality clause*

151. The parties may agree on a post-contract confidentiality clause. Confidentiality obligations may survive the contract, for example, for five-seven years after the contract is terminated or continue indefinitely, depending on the nature of the customer data and other content that was placed in the provider's cloud infrastructure.

- *Post-contract audits*

152. Post-contract audits may be agreed by parties or imposed by law. The contract would need to specify terms for carrying out such audits, including the time frame and allocation of costs.

- *Leftover account balance*

153. The parties may need to agree on conditions for the return to the customer of leftover amounts on its account or for the offset of those amounts against any additional payments the customer would need to make to the provider, including for end-of-the-service activities or to compensate for damage.

M. Dispute resolution

- *Methods of dispute settlement*

154. It is advisable that the parties agree on the method by which future disputes arising out of the contract would be settled. Dispute settlement methods include negotiation, mediation, conciliation, arbitration and judicial proceedings. Different types of dispute may justify different dispute resolution procedures. Disputes over

financial and technical issues, for example, may be referred to a binding decision by a third party expert (individual or body), while some other types of disputes may be more effectively dealt with through direct negotiations between the parties. Law of some jurisdictions may prescribe certain alternative dispute resolution mechanisms that the parties would need to exhaust before being able to refer a dispute to a domestic court.

- *Arbitral proceedings*

155. Disputes that are not amicably settled may be referred to arbitral proceedings, if the parties opted for it. The parties should verify the arbitrability of issues subject to adjudication (i.e., whether the issues to be submitted to adjudication by arbitration are reserved by the State for adjudication by a domestic court). If the parties opted for arbitration, it is advisable for them to agree on a set of arbitration rules to govern arbitral proceedings. A contract can include a standard dispute resolution clause referring to the use of internationally recognized rules for the conduct of dispute resolution proceedings (e.g., the UNCITRAL Arbitration Rules). In the absence of such specification, the arbitral proceedings will normally be governed by the procedural law of the State where the proceedings take place or, if an arbitration institution is chosen by the parties, by the rules of that institution. The parties may opt for an online dispute resolution mechanism with its own set of rules.

- *Judicial proceedings*

156. If judicial proceedings are to take place, due to the nature of **cloud computing services**, several States might claim jurisdiction. Where possible, parties may agree on a jurisdiction clause under which they are obligated to submit disputes to a specific court [cross-link].

- *Retention of data*

157. The contract should address issues of retention of, and access by the customer to, its data and other content for a reasonable period of time, regardless of the nature of the dispute. That may be important for the customer not only because of the need to ensure business continuity but also because access to data, including **metadata** and other **cloud service derived data,** may be vital for dispute resolution proceedings themselves (e.g., to substantiate a claim or counter-claim).

- *Limitation period for complaints*

158. The parties may need to agree on limitation periods within which claims may be brought. The providers may tend to impose relatively short limitation periods for customers to bring claims in respect of the services. Such terms may be unenforceable if they violate mandatory limitation periods stipulated in the applicable law.

N. Choice of law and choice of forum clauses

159. Freedom of contract usually allows parties to choose the law that will be applicable to their contract and to choose the jurisdiction or forum where disputes will be considered. The mandatory law (e.g., data protection law) may however override the choice of law and the choice of forum clauses made by the contracting parties, depending on the subject of the dispute. In addition, regardless of the choice of law and choice of forum, more than one mandatory law (e.g., data protection law, insolvency law) may be applicable to the contract.

- *Considerations involved in choosing the applicable law and forum*

160. Choice of law and choice of forum clauses are interconnected. Whether the selected and agreed-upon law will ultimately apply depends on the forum in which the choice-of law clause is presented to a court or another adjudicating body, e.g., arbitral tribunal. It is the law of that forum that will determine whether the clause is valid and whether the forum will respect the choice of applicable law made by the

parties. Because of the importance of the forum law for the fate of the choice of law clause, a contract with such a clause usually also includes a choice of forum clause.

161. In choosing the forum, the parties usually consider the impact of the chosen or otherwise applicable law and the extent to which a judicial decision made in that forum would be recognized and enforceable in the countries where enforcement would likely be sought. Preserving flexibility in enforcement options may be an important consideration, especially in the **cloud computing** settings where the location of assets involved in the provision of services, the provider and the customer and other factors that parties usually take into account in formulating choice of law and choice of forum clauses may be uncertain.

- *Mandatory law and forum*

162. The law and the forum of a particular jurisdiction may be mandatory on various grounds, for example:

(a) Accessibility of the cloud computing services in the territory of a particular State may be sufficient for application of data protection law of that State;

(b) Nationality or residence of the affected **data subject** or the contracting parties, in particular the **data controller**, may trigger the application of the law of that **data subject** or the party; and

(c) The law of the place in which the activity originated (the location of the equipment) or to which the activity is directed for the purpose of extracting benefits may trigger the application of the law of that place. The usage of the geographic domain name associated with a particular place, the local language used by the provider in its web design, pricing in local currency and local contact points are among factors that might be taken into account in making such determination.

- *Provider or customer home law and forum*

163. Contracts for **standardized commoditized multi-subscriber cloud solutions** often specify that they are governed by the law of the cloud provider's principal place of business or place of establishment. They typically grant the courts of that country exclusive jurisdiction over any disputes arising out of the contract. The customer may prefer to specify the law and jurisdiction of its own country. Public institutions generally would have significant restrictions on their ability to consent to the law and jurisdiction of foreign countries. Providers that operate in many jurisdictions may be flexible as regards the choice of the law and forum of the country where the customer is located.

- *Multiple options*

164. The parties may also specify various options for different aspects of the contract. They may also opt for a defendant's jurisdiction to eliminate the home forum advantage for a plaintiff and thus encourage informal resolution of disputes.

- *No choice of law or forum*

165. Some parties may prefer no choice of law or forum clause in their contract, leaving the question open for later argument and resolution if and when needed. That might be considered the only viable solution in some cases.

O. Notifications

166. Notifications clauses would address the form, language, recipient and means of notification, as well as when the notification becomes effective (upon delivery, dispatch or acknowledgment of receipt). In the absence of any mandatory legislative provisions, parties may agree upon formalities for notification, which could be uniform or vary depending on the level of importance, urgency and other considerations. More stringent requirements would be justified, for example, in case of suspension or unilateral termination of the contract, as compared to routine

notifications. Deadlines in such cases should allow for **reversibility** and customer business continuity. The contract may contain references to any notifications and deadlines imposed by law.

167. The parties may opt for **written** notification to be served at the physical or electronic address of the contact persons specified in the contract. The contract may specify the legal consequences of a failure to notify and of a failure to respond to a notification that requires a response.

P. Miscellaneous clauses

168. Parties often group under miscellaneous clauses provisions that do not fall under other parts of the contract. Some of them may contain a standard text appearing in all types of commercial contracts (so called “boilerplate provisions”). Examples include a severability clause allowing removing invalid provisions from the rest of the contract or a language clause identifying a certain language version of the contract as prevailing in case of conflicts in interpretation of various language versions. Placing contractual clauses among miscellaneous provisions does not diminish their legal significance. Some of them may need to be carefully considered by the parties in the light of cloud computing specifics.

Q. Amendment of the contract

169. Amendments to the contract could be triggered by either party. The contract would address the procedure for introducing amendments and making them effective. The contract may also need to address the consequences of rejection of amendments by either party.

170. In the light of the nature of **cloud computing**, it might be difficult to differentiate changes that would constitute amendment of the contract from those changes that would not. For example, the customer’s use of any options made available from the outset in the contract would not necessarily constitute an amendment of the initial contract, nor would changes in services resulting from routine maintenance and other activities of the provider covered by the contract. The addition of any features not covered by the originally agreed terms and thus justifying changes in price may, on the other hand, constitute amendment of the contract. Any updates leading to material changes to previously agreed terms and policies may also constitute an amendment of the contract. Substantial modifications to the material terms of the originally concluded contract (e.g., discontinuation of some cloud computing services) may effectively lead to a new contract.

171. The extent of permissible modifications to public contracts may be limited by public procurement rules that usually restrict the freedom of parties to renegotiate terms of a contract that were subject to public tendering proceedings.

172. In the light of frequent modifications of the originally agreed terms, each party may wish to store independently of each other the complete set of the originally agreed terms and their modifications.

Glossary

Acceptable use policy (AUP) — part of the cloud computing contract between the provider and the customer that defines boundaries of use by the customer and its end-users of the cloud computing services covered by the contract, e.g., that the customer and its end-users shall not place and use any illegal or other prohibited content in the cloud [cross-link].

Audit — the process of examining compliance with contractual and statutory requirements. It may cover technical aspects, such as quality and security of hardware and software; compliance with any applicable industry standards; and the existence of adequate measures, including isolation, to prevent unauthorized access to and use of the system and to assure data integrity. It may be internal by the provider or external by the customer or by an independent third party appointed by either the provider, the customer or both.

Cloud computing — supply and use of **cloud computing services** through open or closed network. It may be characterized by:

(a) **Broad network access,** meaning that **cloud computing services** 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,** meaning metered delivery of **cloud computing services** as in the public utilities sector (gas, electricity, etc.), allowing usage of the resources to be monitored and charged by reference to level of usage (on a **pay-as-you-go** basis);

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

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

(e) **Elasticity and scalability,** meaning the capability for rapidly scaling up or down the consumption of **cloud computing services** according to customer's needs, including large-scale trends in resource usage (e.g., seasonal effects). Elasticity and scalability encompass not only quantitative aspects of the service but also the quality and security of the measures, that may need to be adapted to the varying sensitivities of the stored customer data;

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

Cloud computing services — services provided via **cloud computing**. They vary and constantly evolve. They may include the provision and use of simple connectivity and basic computing services (such as storage, emails and office applications). They may also include the provision and use of the whole range of physical information technology (IT) infrastructure (such as servers and data centres) and virtual resources needed to build own IT platforms, or deploy, manage and run customer-created or customer-acquired applications or software. **IaaS, SaaS, PaaS**, etc., are all types of cloud computing services.

Cloud computing service partners (e.g., cloud auditors, cloud service brokers or system integrators) — persons engaged in support of, or auxiliary to, activities of either the provider or the customer or both. Cloud auditors conduct an **audit** of the provision and use of **cloud computing services**. Cloud service brokers assist parties with a wide range of issues, e.g., with finding the right cloud solution, negotiating acceptable terms and migrating the customer to the cloud.

Cloud service derived data — data under control of the provider that is derived as a result of the use by the customer of the cloud computing services of that provider. It includes **metadata** and any other log data generated by the provider containing records of who used the services, at what times, which functions and the types of data involved. It can also include information about authorized users, their identifiers, any configuration, customization and modification.

Data controller — a person that determines the purposes and means of the processing of **personal data**.

Data localization requirements — requirements relating to the location of data and other content or data centres or the provider. They may prohibit certain data (including **metadata** and backups**)** from residing or transiting in or out of a certain area or jurisdiction or require prior approval to be obtained from a competent State body for that. They are often found in data protection law and regulations, which may in particular prohibit **personal data** from residing or transiting in jurisdictions that do not adhere to certain standards of **personal data** protection.

Data processor — a person that processes the data on behalf of the **data controller**.

Data subjects' rights — rights associated with data subjects' **personal data**. Data subjects under law may enjoy the right to be informed about all significant facts related to their personal data, including its location, use by third parties and data leaks or other data breaches. They may also have the right to access their personal data at any time, the right to erasure of their personal data (pursuant to the right to be forgotten), the right to restrict **processing** of their personal data and the right to **portability** of their personal data.

Deployment models — various ways in which cloud computing is organized based on the control and sharing of physical or virtual resources:

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

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

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

(d) **Hybrid cloud** where at least two different cloud deployment models are used.

Downtime or outages — the time when the cloud computing services are not available to the customer. That time is excluded from the calculation of **uptime** or availability. Time for maintenance and upgrades is usually included in downtime.

First response time — the time between the customer reporting an incident and the provider's initial response to it.

Follow-the-sun — a model in which the workload is distributed among different geographical locations to more efficiently balance resources and demand. The purpose of the model may be to provide round-the-clock services and to minimize the average distance between servers and end-users in an effort to reduce **latency** and maximize the speed with which data can be transmitted from one device to another (data transfer rate (DTR) or throughput).

IaaS — types of **cloud computing services** with which the customer can obtain and use processing, storage or networking resources. The customer does not manage or control the underlying physical or virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical or virtual resources. The customer may also have limited ability to control certain networking components (e.g., host firewalls).

Insolvency representative — a person or body authorized in insolvency proceedings to administer the reorganization or the liquidation of the assets of the insolvent provider that are subject to the insolvency proceedings.

Interoperability — the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

IP licences — agreements between an IP rights owner (the licensor) and a person authorized to use those IP rights (the licensee). They usually impose restrictions and obligations on the extent and manner in which the licensee or third parties may use the licenced property. For example, software and visual content (designs, layouts and images) may be licensed for specific use, not allowing copying, modification or enhancement, and be restricted to a certain medium. The licences may be limited to a particular market (e.g., national or (sub)regional), number of users or may be time-bound. Sub-licensing may not be permitted. The licensor may require reference to be made to the IP rights owner each time the IP rights are used.

Latency — from the customer's perspective, the delay between a user's request and a provider's response to it. It affects how usable the **cloud computing services** actually are.

Layered cloud computing services — where the provider is not the owner of all or any computing resources that it uses for provision of the cloud computing services to its customers but is itself the customer of all or some **cloud computing services**. For example, the provider of **PaaS** or **SaaS** types of service may use storage and server infrastructure (data centres, data servers) owned or provided by another entity. As a result, one or more sub-providers may be involved in providing the cloud computing services to the customer. The customer may not know which layers are involved in the provision of services at a given time, which makes identification and management of risks difficult. **Layered cloud computing services** are common in particular in **SaaS**.

Lock-in — where the customer is dependent on a single provider because costs of switching to another provider are substantial. Costs in this context are to be understood in the broadest sense as encompassing not only monetary expenses but also effort, time and relational aspects. Risks of application and data lock-ins may be high in **SaaS** and **PaaS**. Data may exist in formats specific to the provider's cloud system that will not be usable in other systems. In addition, the provider may use a proprietary application or system to organize customer's data requiring adjustment of licensing terms to allow operation outside the provider's network. In **PaaS**, there could also be runtime lock-in since runtimes (i.e., software designed to support the execution of computer programs written in a specific programming language) are often heavily customized (e.g., such aspects as allocating or freeing memory, debugging, etc.). **IaaS** lock-in varies depending on the specific infrastructure services consumed, but may also lead to application lock-in if there is dependence on specific policy features (e.g., access controls) or data lock-in if more data is moved to the cloud for storage.

Metadata — basic information about data (such as author, when the data was created, when it was modified and file size). It makes finding and using the data easier and may be required to ensure the authenticity of the record over time. It can be generated by the customer or the provider.

PaaS — types of **cloud computing services** with which the customer can deploy, manage and run in the cloud customer-created or customer-acquired applications using one or more existing programing languages and execution environments supported by the provider.

Performance parameters — quantitative (with numerical targets or metrics or performance range) or qualitative (with service quality assurances) parameters. They may refer to conformity with applicable standards, including the date of expiry of any conformity certification. To be meaningful, they would aim at measuring performance that is important to the customer and should do so in an easy and auditable way. They

could be different depending on the risks involved and business needs (e.g., the criticality of certain data, services or applications and the corresponding priority for recovery). For example, a non-mission critical system that is designed to use the cloud for archival purposes will not need the same **uptime** or other **SLA** terms as mission critical or real-time operations.

Persistency of data storage — the probability that data stored in the cloud will not be lost during the contract period. It can be expressed in the contract as a measureable target against which the customer will measure steps taken by the provider to ensure persistency of data storage.

Personal data — data that can be used to identify the natural person to whom such data relates. The definition of personal data in some jurisdictions may encompass any data or information directly or indirectly linked or relating to an identified or identifiable individual (the **data subject**).

[Personal data] processing — collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, of data.

Portability — ability to easily transfer data, applications and other content from one system to another (i.e., at low cost, with minimal disruption and without being required to re-enter data, re-engineer processes or re-program applications). This might be achieved if it is possible to retrieve the data in the format that is accepted in another system or with a simple and straightforward transformation using commonly available tools.

Post-incident steps — measures to be taken after a security incident by the provider, the customer or both, including by involving a third party. They may include isolation or quarantine of affected areas, performance of root cause analysis and production of an incident analysis report by the affected party or jointly with the other party or by an independent third party.

Recovery point objectives (RPOs) — the maximum time period prior to an unplanned interruption of services during which changes to data may be lost as a consequence of recovery. If RPO is specified in the contract as two hours before the interruption of services, that would mean that all data would be accessible after recovery in the form it existed two hours before the interruption occurred.

Recovery time objectives (RTO) — the time frame within which all cloud computing services and data must be recovered following an unplanned interruption.

Reversibility — process for the customer to retrieve its data, applications and other related content from the cloud and for the provider to delete the customer data and other related content after an agreed period.

SaaS — types of **cloud computing services** with which the customer can use the provider's applications in the cloud.

Sector specific regulation — financial, health, public sector or other specific sector or profession regulations (e.g., attorney-client privilege, medical professional secrecy) and rules for handling classified information (broadly understood as information to which access is restricted by law or regulation to particular classes of persons).

Security incident notification — a notification served to affected parties, State authorities or the public at large about a security incident. It may include circumstances and the cause of the incident, type of affected data, the steps to be taken to resolve the incident, the time at which the incident is expected to be resolved and any contingency plan to employ while the incident is being resolved. It may also include information on failed breaches, attacks against specific targets (per customer user, per specific application, per specific physical machine), trends and statistics.

Service level agreement (SLA) — part of the cloud computing contract between the provider and the customer that identifies the cloud computing services covered by the

contract and how they should be delivered (the **performance parameters**) [cross-link].

Standardized commoditized multi-subscriber cloud solutions — cloud computing services provided to an unlimited number of customers as a mass product or commodity on non-negotiable standard terms of the provider. Broad disclaimers and waivers of provider's liability are common in this type of solution. The customer may be in a position to compare different providers and their contracts and select among those available on the market the most suitable for its needs, but not to negotiate a contract.

Uptime — time when the cloud computing services are accessible and usable.

Written or **in writing —** information that must be accessible so as to be usable for subsequent reference. It encompasses information on paper and in an electronic communication. "Accessible" means that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. "Usable" covers both human use and computer processing.