ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Read Before Signing: 15 Terms in Cloud Service Agreements

Technology, Privacy, and eCommerce

More law departments are making the move to the cloud. Previously, we discussed the basics of cloud computing, from the different categories of services to data management. Before implementing a new cloud service, learn these terms that appear in these tech-heavy agreements.

1. Minimum standards: availability, speed of performance, and communication

One of the most important concerns in a cloud computing arrangement is the performance of the cloud services, and whether they meet the customer's needs in terms of reliability and quality.

The agreements will set forth the minimal requirements with respect to:

- Uptime or availability of the services;
- Quality or accuracy of the deliverables; and
- Service level escalation matrix (performance failure severity levels, and response/resolution deadlines).

CSP will often attempt to exclude uptime and availability requirements for routine maintenance, emergency work, and force majeure events. Further, CSPs elect to omit resolution deadlines and expand force majeure beyond commonly accepted incidents. No CSP can guarantee 100 percent availability, due to the nature of the cloud services.

2. Change of services

CSP frequently include a unilateral right to modify the terms and conditions in their contracts in order to avoid bilateral renegotiation on a contract-by-contract basis.

3. Remedies

Cloud computing contracts typically limit legal remedies available to the customer to minimize liability and reduce costs.

Remedies usually consist of repairs (fixing technical glitches), credits on the next invoice, or other remedies for service failures. Normally refunds are not available for this breach. There is little room for negotiation in these agreements because the services are highly standardized, and there are technical limitations to what the CSP can accommodate for each individual customer.

However, the customer should be able to obtain actual damages and termination rights for repeated and severe failures. Finally, it would be in the customers' interest to demand their CSPs conduct root cause analysis to avoid any future failures.

4. Deadlines for acknowledgment

These contracts usually provide deadlines by which the CSP needs to acknowledge requests from the customers to support or to fix a problem.

5. Warranties

Depending on the negotiations, the customers may demand the CSP to warrant that the service:

- Will be performed in accordance with the specifications,
- Will not infringe any intellectual property rights of any third party, and
- Will not contain or transmit any computer virus or other harmful code.

CSPs seek to limit warranties to the warranty of function (i.e., that the technology will work as described in the specifications). Warranty is customarily considered as sole and exclusive remedy for breach of the warranty of function.

Where the CSP makes such a promise to a customer, it would be in its best interest to emphasize that "the technology will work in material conformity with the technical specifications attached to this contract." Minor errors or glitches should not be considered as malfunction.

Warranty clauses usually come with an expiry date. The CSP will not warrant that the technology will work indefinitely; it will have a start date and an end date.

Remedies clauses (for example the provider giving credit to the customer in case of a failure to

perform) and warranty clauses are usually mutually exclusive. Which remedy to choose — credit or warranty — would be subject to negotiation between the parties.

6. Intellectual property ownership

These clauses provide that the CSP has all the rights to the technology and that a third party will not sue customers for breach of intellectual property rights. However, these clauses should not be needed in cloud contracts, because the customer does not receive a copy of the software.

7. Maintenance

If the server and software are hosted for a specific customer, the CSP may have to provide the maintenance services (i.e., repair the technology). Most of the time, this will mean that the CSP will make reasonable efforts to keep the technology working. Maintenance clauses are more likely to be encountered in IaaS and PaaS contracts.

It is not unusual for CSPs to display their standard maintenance plans on their website, and for some contracts to include provisions for upgrades and updates — so long as the customer pays for them. Usually, customers will not pay for minor upgrades (where the upgrade corrects minor bugs), but if the upgrade provides new features, then the CSPs will be likely to charge for it.

8. Acceptance, rejection, and delivery

Cloud service agreements identifying deliverables will describe conditions for acceptance, rejection, and delivery. These clauses allow the customer to test the technology to see if it works. If the services fail the test, the customer will have the right to reject, and the CSP will be required to refund.

It is important to note that the customers do not have the right to reject the service just because it did not meet their expectations. For the customer to be able to reject the services, they must not be conforming to the written specifications.

9. Audit rights

Some customers ask for the right to evaluate the CSP’s security system. Usually, CSPs refuse customer led audits, preferring instead periodic independent audits. CSPs are more likely to accept independent auditing companies to audit them than the customers themselves, because they are worried about protecting their other customers’ data.

Some agreements refer to independent auditing requirements, based on standards such as the American Institute of Certified Public Accountants (AICPA).

These are the most relied-upon standards for reporting on data security. AICPA’s Service Organization Control (SOC 2) reports use the AICPA’s attestation standards.

Most contracts will exclude consequential damages.

This is not the only auditing option for customers, but each organization's IT department's security experts could decide on what standards to use. There are also the ISO 27001 audit standards for testing technical data security levels. SOC 2 is mostly encountered in contracts with American parties, and ISO 27001 seem to be the preferred standards for Europeans.

10. Limitation of liability and exclusion of consequential damages

Almost all cloud computing contracts contain a limitation of liability clause heavily weighted in favor of the CSP; customers accept these clauses in light of the more immediate benefits, like cost savings and scalability. Most limitations consist of capping the CSP's liability at the amount they receive from the customer.

Some courts may refuse to enforce the limitations of liability clauses if it is determined that the customer did not understand the importance of the clause. This explains why most limitation of liability clauses are capitalized.

Most contracts will exclude consequential damages.

The indemnification provisions require the CSPs to hold the customer harmless against losses caused by their breach of representations, gross negligence, and willful misconduct. Most of the time, the limitation of liability provisions will exclude the indemnity obligations.

Moving to the Cloud? Know the Basics Before Contracting

Parties frequently negotiate data breach indemnification language. Broader indemnification language benefits the customer while CSP will attempt to limit its responsibility.

11. Training clause

Most cloud computing contracts contain a clause requiring the CSP to teach the customer how to use the technology.

12. Disaster recovery clause

The legal counsel should pay attention to the descriptions of the agreements' force majeure provisions as well as the provider's recovery and business continuity program. These clauses set out recovery procedures for disasters (e.g., wars, natural disasters, etc.).

> If the upgrade provides new features, then the CSPs will be likely to charge for it.

Customers should identify force majeure events called out in the contract and object where outside conventional understanding. Excusal of the CSP from performance should hinge upon compliance with their business continuity plan.

The cloud services agreements should also specifically address what will happen in the event of prolonged down-time because of a force majeure event or failure of the business continuity plan.

In addition to customary termination rights, the customer may want to negotiate for “step-in rights” that would allow it to take over (or have a new CSP to take over the services during the force majeure period, with the CSP paying any difference in fees between the actual costs to the customer and the negotiated fees in the original cloud services agreement.

13. Insurance clauses

Almost all cloud agreements will impose customary insurance obligations on the CSPs. Increasingly, customers solicit specialized insurance coverage for data breaches, network attacks, denial of service, website defacement, online blackmail, and IP claims.

14. Interoperability

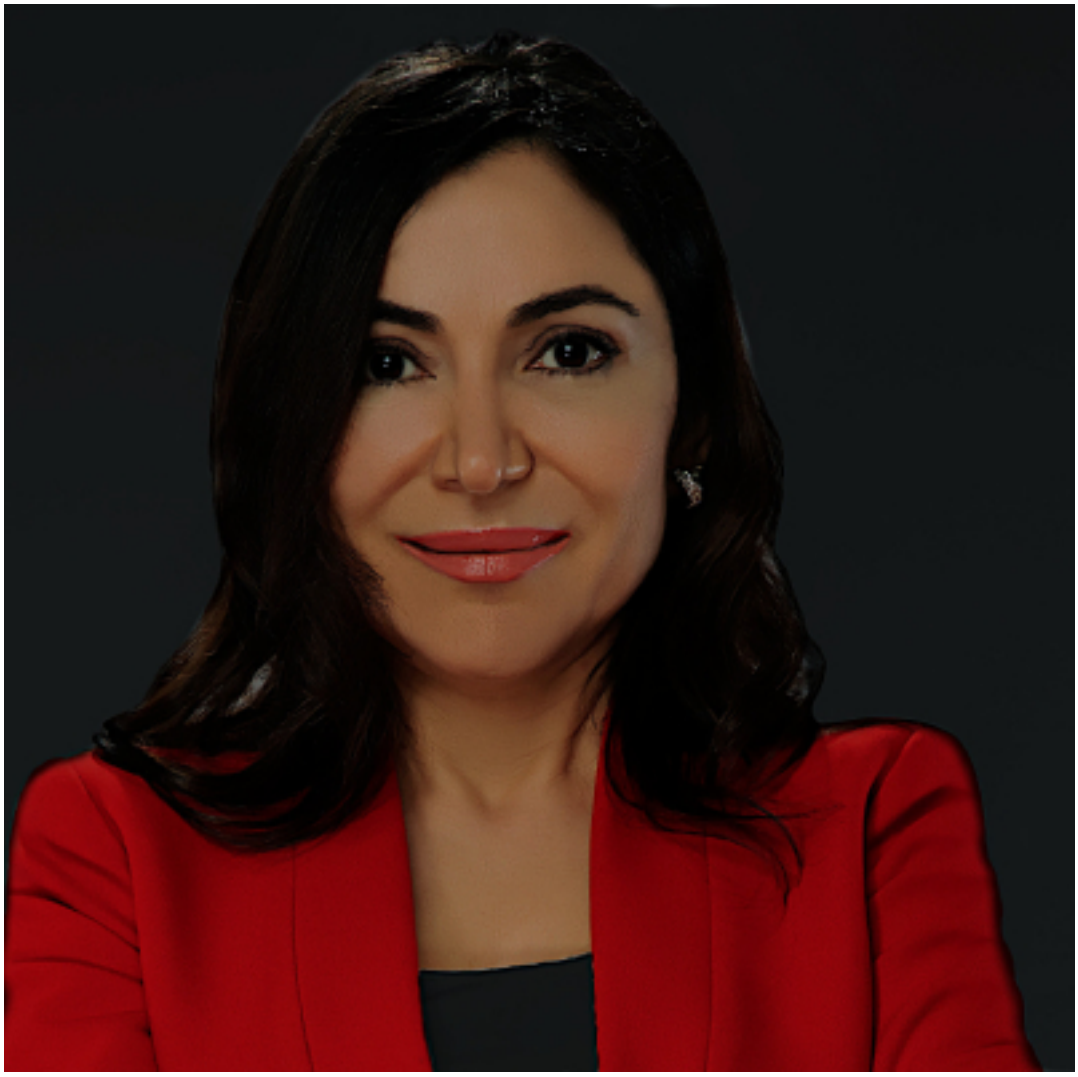
Without current, uniform cloud computing standards, it falls to customers to consider compatibility and interoperability between CSPs before contract award, or risk disruption and added expense in the event of transition.

15. Termination

The agreements will define customers’ termination rights, typically for events directly impacting continued performance. This includes, for example, merger or acquisition of the CSP or financial distress (i.e., bankruptcy). Customer termination clauses should also address transition of the CSP’s contracted duties to migrate data and minimize disruption.

To avoid risks of unauthorized access or breach of data, the CSP should return or destroy the customer's data upon termination or expiration of the agreement. Most cloud service providers seek to retain anonymized, aggregated data to improve their services. Customer privacy policies and local privacy regulations may impose additional, often unique burdens bearing incorporation into cloud agreements.

Laura Reynaud



Senior Legal Counsel

Siemens

Laura Reynaud is senior legal counsel at Siemens. She is a US-qualified corporate and commercial lawyer with 13 years of experience in the Middle East. Reynaud specializes in commercial contracts, mainly technology contracts, IP, cybersecurity, cloud computing, and data protection. Reynaud holds an LLM focused in International Corporate and Commercial Law from King's College London. She is based in Saudi Arabia.