CloudWATCH
Contractual Clauses in Cloud Contracts

A Cloud Service Agreement (CSA) consists of a set of documents governing the relationship between the cloud service provider and the customer. While cloud computing technology is evolving at a fast pace, the same cannot be said for contracts in the cloud context. Due to the usual imbalance between the size of the cloud provider and that of the cloud customer, CSAs are generally offered by cloud providers in standard, non-negotiable, "take it or leave it" terms.

This context makes it difficult for cloud customers to ensure that they can discharge the duties imposed on them by EU legislation with regard to privacy and data protection. The difficulty is accentuated by the fact that, although CSAs are similar in nature, there is no standard CSA "template" that customers could refer to as a guide for understanding what clauses they are expected to find in a CSA or for comparing a cloud service offer with the standard provided. Therefore, we have identified some sample clauses that consumers can expect to find in CSAs, in order to give readers a starting point for understanding the content of a cloud contract and the typical approach that cloud service providers take with regard to the various contractual aspects; the clauses indicated below must be read as different approaches to discipline a certain contractual issue.

The clauses have been drafted from the perspective of a customer SMEs. However, they may constitute a good starting point for Public Authorities as well, save what is provided for them by specific legislation applicable to them, which needs to be carefully assessed on a case by case basis.

The sample clauses are for illustrative purposes only and do not constitute legal advice; all references to places, names, factual circumstances are purely coincidental.

1. Identification of the contracting parties – Commonly found clauses

a. *This Cloud Services Agreement is between the Provider, an entity established in … (e.g. France) - and the individual or entity that has executed this Agreement ("You").*

b. *This Agreement is made and entered into by and between the Provider and the entity agreeing to these terms ("Subscriber").*

c. *Using this agreement, the Customer may subscribe to Cloud Services. This agreement and the applicable Annexes and the related Documents form the entirety of this Contract.*

Check closely the entities involved

Even though many people tend to believe that the initial part of a cloud service contract is only a formality of stating the two parties involved, it is actually important to pay attention

to it because it **reveals an essential detail: the specific entity that the cloud service customer is contracting with and other information related to it, such as its location.** Some cloud service providers have set up affiliates in Europe (see *example a* above), in which case the customer is contracting with a EU-based entity and the contract is very likely subject to the law of the Member States where the specific affiliate is established. In other cases, the customer is contracting directly with the affiliate's holding company, which is often located outside the EU. Therefore, issues concerning the data protection law applicable to the personal data processing – and specifically to the transfer of personal data - will have to be critically assessed.
In addition, this introductive clause provides information about the other documents or annexes that may form part of the agreement, thus giving an overview of the entire contractual relationship. For example, you can find information regarding the hierarchy of the Cloud Service Level Agreement, the Privacy Level Agreement and specific Service Orders for additional services.

2. Subprocessors and subcontractors – Commonly found clauses

a. *The provider may use processors and subprocessors, including personnel and resources, in various locations around the world to deliver the Cloud Services. The Client's personal data may be transferred across country borders including outside the European Economic Area (EEA). A list of countries where the Client's content may be processed is available in Attachment [___] (e.g. Privacy and Data Protection Terms). Other information related to data processing is available upon request.*

b. *Some or all of the Provider's obligations under the Agreement may be performed by the Provider's Affiliates, who have entered into an intra-company agreement under which the Provider's Affiliates Processing Personal Data adopt safeguards consistent with those of the Provider. In addition, the Provider may engage subcontractors to assist in the provision of the Cloud Services. The Provider will provide a copy of the list of subcontractors to the Customer upon request.*

Legal implications of the personal data transfers to subprocessors

Cloud services very often entail the processing of personal data on servers located outside the European Union, since some of the main providers of cloud services are either based outside the EU or use infrastructure outside the EU. Therefore, personal data uploaded to the cloud is very likely to be transferred to entities located outside the EU.
Art. 28 (1) of the new General Data Protection Regulation 679/2016 provides that controllers must only use processors providing sufficient guarantees "*to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*". Moreover, processing should be covered by a specific controller-processor agreement whereby the processor is held to comply with specific legal rules in order to guarantee an acceptable level of data protection.

Another way to legally transfer data from a controller to a processor is by using standard contractual clauses binding both parties to specific privacy obligations. The current standards are available on the website of the European Commission at the following link: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.
Other innovations brought by the new Regulation 679/2016 are specific certifications and codes of conduct, which will enable controllers and processors to certify that they comply with a particular level of data protection. Art. 28 (5), in particular, sets out that "*Adherence of a processor to an approved code of conduct […] or an approved certification mechanism […] may be used as an element by which to demonstrate sufficient guarantees […]*".
It is strongly recommended to check whether the cloud service provider has procedures in place to ensure that the data is transferred to its subprocessors on a valid legal basis and that the subprocessors it engages can prove their adherence to the data protection rules set out by the new Regulation. In this regard, the clause b) reported above seems to be more in line with what set out by applicable data protection law.

3. Modifications to the CSA – Commonly found clauses

a. *If the Provider makes a material change to the Services, the Provider will inform Customer, provided that Customer has subscribed with the Provider to be informed about such change. The Provider may make modifications to this Agreement from time to time. Material modifications shall become effective 30 days after they are posted, except if the modifications apply to new functionality in which case they will be effective immediately. If the Customer does not agree to the revised Agreement, the Customer must stop using the Services.*

b. *The Provider may change the Terms related to data processing and security services where such modification is required to comply with applicable law, applicable regulation, court order, or guidance issued by a governmental regulator or agency, or where such change is commercially reasonable, does not result in a degradation of the overall security of the Services, and does not otherwise have a material adverse impact on Customer's rights under the Terms.*

c. *The Provider may reasonably modify a Cloud Service, without degrading its functionality or security features. Any change that affects the commercial terms (e.g. charges) of the Cloud Service will not be effective until the next agreed renewal or extension. Client accepts changes by placing new orders or continuing use after the change effective date or allowing transactions to renew after receipt of the change notice. Except as provided above, all changes to the Agreement must be in writing accepted by both parties.*

Keep an eye out for changes in terms and conditions

Some recurring "keywords" are often found in clauses addressing the situations in which an agreement may be modified. One such keyword, as may be noted above, is "reasonable" or "commercially reasonable". These give the cloud service provider a relatively wide margin for

identifying circumstances when changes may be applied, sometimes without notifying the consumer. However, the same keyword ("reasonable") can also be a powerful tool for the informed customer to dispute whether the circumstances of the modifications are objectively reasonable.

More importantly, as noted in the examples above, customers are well advised to keep up to date with any potential changes by regularly checking the Terms and Conditions or the Service Level Agreement links on the chose provider's website.

Changes must usually be made in writing, but as can be seen above, both parties don't always have to accept them for them to be valid. Sometimes, as in example a), the changed agreement will simply be posted on the cloud service provider's website.

4. Term and Termination; Effect of Termination – Commonly found clauses

a. *The Provider may withdraw a Cloud Service on 12 months' notice, unless otherwise stated in an Attachment. The Provider will either continue to provide the Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another the Provider Service. Customer may terminate this Agreement for its convenience at any time on prior written notice and upon termination, must cease use of the applicable Services. The Provider may terminate this Agreement for its convenience at any time without liability to Customer.*

b. *If the Agreement is terminated, then: (i) the rights granted by one party to the other will immediately cease; (ii) all Fees owed by Customer to the Provider are immediately due upon receipt of the final electronic bill; (iii) Customer will delete the Software, any Application, Instance, Project, and any Customer Data; and (iv) upon request, each party will use commercially reasonable efforts to return or destroy all Confidential Information of the other party.*

c. *Following termination of the Cloud Services, the Provider will return or otherwise make available for retrieval Customer's Personal Data available in the Customer's Cloud Services environment. Following return of the data, or as otherwise specified in the Agreement, the Provider will promptly delete or otherwise render inaccessible all copies of Personal Data from the production Cloud Services environment, except as may be required by law.*

Maintaining control over personal data when the cloud contract ends

Cloud Service Agreements usually include terms regarding the circumstances and effects of a termination. The customer should always check the notice that must be given by each party in order to effectively terminate the agreement. Sometimes the notice period that the provider must give differs from that which the customer must give.

It is also vital to check how (and when) the customer's data will be returned by the provider. **Pay attention to the difference in the choice of words**, as the specific meaning can have significant implications for the Customer's access to their own data following the termination of the cloud service agreement. If we compare the use of "commercially reasonable efforts"

to return the information with "will return or otherwise make available for retrieval" the information you can see two different approaches that can have very different consequences for the Client's access to data following the termination of the CSA.
It is essential to receive reliable evidence of complete deletion of personal data upon termination of the contract.

5. Data Location – Commonly found clauses

a. *Customer may select where certain Customer Data will be stored and the Provider will store it there in accordance with the Service Terms. Where necessary, the Provider may process and store the Customer Data anywhere the Provider or its agents have facilities. Under this Agreement, the Provider is merely a data processor.*

b. *Where the Provider's Affiliates or Subprocessors are located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission pursuant to Articles 25(6) and 31(2) of the Directive or by a competent national data protection authority, data transfers are managed as follows. Transfers from Customer to the Provider or the Provider's Affiliates are made subject to the terms of this Data Processing Agreement and (i) the Model Clauses, with Customer acting as the "data exporter" and the Provider and/or the Provider's Affiliate (s) acting as the "data importer(s)" (as those terms are defined in the Model Clauses); or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the applicable requirements of Articles 25 and 26 of the Directive. The terms of this Data Processing Agreement shall be read in conjunction with the Model Clauses or other appropriate transfer mechanism referred to in the prior sentence.*

Check where data will be located

The place where personal data may be processed within a cloud environment is critical because **personal data transfers to countries outside the EU must follow the rules** set out in Articles 25 and 26 of the Directive 95/46/EC, as well as in Chapter V of the Regulation 2016/679 (General Data Protection Regulation).
The Provider could use any of its affiliates to process and store the customer's data, and this is why the customer should pay attention to the location of such affiliates and to the mechanisms put in place by the Provider, in order to ensure that the data transfer and the subsequent storage of the data are conducted in compliance with the applicable laws.

6. Data Security - Commonly found clauses

a. *The Customer is responsible for any security vulnerabilities, and the consequences of such vulnerabilities arising from Customer Content and Customer Applications, including any viruses, Trojan horses, worms or other programming routines contained in*

Customer Content or Customer Applications that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data.

b. *The Attachment for each Cloud Service describes the security functions and features of the Cloud Service. By using the Cloud Service Client acknowledges that it meets Client's requirements and processing instructions.*

How will your data be kept secure?

Pursuant to Article 28 (3) of the General Data Protection Regulation 2016/679, the Data Processor has the obligation to take all the measures contained in Article 32 ("Security of Data"). Article 32 includes a set of rules referring to **pseudonymysation and encryption, ensuring confidentiality, integrity, availability and resilience, as well as ensuring access to data in the event of a technical or physical incident**. In addition, Article 33 of the same Regulation also lays down the steps that need to be taken in the event of a **data breach**. For example, notifying the customer and describing the consequences of the breach, as well as steps to be taken to mitigate potential adverse effects of a data breach.

On top of the minimum required security measures, each Processor may offer additional, customizable security features in order to gain a competitive advantage over other Processors. Such additional security features could be taken into account when choosing the preferred cloud service provider.

7. Limitation of Liability - Commonly found clauses

a. *To the maximum extent permitted by applicable law, neither party, nor the Provider's suppliers, will be liable under this agreement for lost revenues or indirect, special, incidental, consequential, exemplary, or punitive damages, even if the party knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.*

b. *The Provider's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim. This limit applies collectively to the Provider, its subsidiaries, contractors, and suppliers. The Provider will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.*

Check how the provider limits its liability

Cloud contracts typically contain clauses whereby liability is excluded as much as legally possible. However, it is important to note as, in *example b*, the limitation on the amount that may be paid cannot exceed the amount paid by the customer in the 12 months preceding the event that entitled the customer to damages. However, such a cap is not always set at the same threshold and may vary amongst providers. Cloud customers are

advised to **check how the cloud service provider limits its liability** and to take this factor into account when making a decision and signing an agreement.

8. Jurisdiction and Applicable Law; Compliance with EU Law

a. Both parties agree to the application of the laws of the State of [___] (e.g. Michigan, United States), without regard to conflict of law principles. The rights and obligations of each party are valid only in the country of Client's business address. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect.

b. This Agreement is governed by [___] (e.g. German law) and the Parties agree to submit to the exclusive jurisdiction of, and venue in, the courts of [___] (e.g. Germany) in any dispute arising out of or relating to this Agreement.

Watch out for law applied to the contract and law applied to personal data processing

On the concept of **applicable law**, **a distinction** has to be made **between the law applying to the contract and regulating its interpretation, and the law applicable to personal data processing.** The former may usually be contractually agreed by the parties; the latter may not be agreed upon by the parties, as it follows criteria set out in public imperative law.
For example, Article 3 (1) of the new General Data Protection Regulation 679/2016 establishes that the *"Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."* Moreover, Article 3 (2) further sets out that the Regulation also applies where the Controller or Processor are located outside the EU and either they offer goods or services in the Union, or monitor the behavior of people located in the EU. Therefore, the Regulation has a wide scope of application.
In the case just explained, where the conditions provided for by the law are met, EU law applies to it regardless of any other different arrangement agreed upon by the parties.