**Free translation**

# CLOUD CONTRACTS AND PRIVACY

The fire that broke out in the night between 9 and 10 March at the OVH data centre in Strasbourg had direct and important consequences for many companies and public administrations, including Italian ones, with websites off-line and the impossibility of using the services and accessing the data contained in the cloud. In Italy, for example, the municipalities of Pavia, Trapani and Cattolica were affected; in France, the Pompidou national art centre, but also, in the rest of Europe, the blogging and cryptocurrency exchange platform Deribit and the news agency eeNews Europe, and many others.

The incident – whose consequences and duration are still unclear at the moment (OVH has promised to restart its data centre between 15 and 19 March, with a full recovery in the following two weeks) – has put the spotlight back on so-called cloud computing, which is very convenient and useful for companies, both public and private, but has critical profiles and risks in the area of data protection, due to the danger of losing control of one's own data; it is therefore useful to recall the precautions that shall be taken when entering into the contract with the service provider and the possible consequences, including penalties, of violating EU Regulation 2016/679 (GDPR).

From a data protection point of view, the public body or private company that uses an external provider of cloud services and processes the data of natural persons (their customers or users) are qualified as "Data Controllers" and shall designate the provider of such services as "External Data Processor" pursuant to Article 28 of GDPR; the Data Controller shall pay particular attention to this contractual phase, not only by including all the clauses provided as mandatory by the aforementioned Article 28, but also by taking care to verify that the guarantees and security measures offered by the provider are suitable for data protection.

This is done with a view to both safeguarding one's own corporate data (whether personal or non-personal), which in many cases represent a company's most important asset, and to avoiding possible sanctions: it should be remembered that, in the event of violations committed by the cloud system provider, the Data Controller will also be called upon to answer for any wrongdoing.

It is true that often the Data Controllers, especially if small, do not have such contractual power as to allow them to require the cloud provider to include in the standard contract (usually unilaterally drafted) special clauses and guarantees as well as additional security systems and measures. It should be noted, however, that this objective fact does not exempt the Data Controller from possible liability in the event of a breach of the privacy legislation: Data Controller always has the possibility to, and indeed must, turn to the supplier that offers greater guarantees.

In the contractual phase and when drafting the appointment of a supplier as External Data Processor, the Data Controller shall therefore carefully check what security measures are adopted by the supplier (in this case, a cloud provider) to protect the data: in this regard, the supplier generally has protection systems in place against viruses, hacker attacks or other cyber threats. The OVH case has, however, taught us that one shall never forget the physical security of the places where the computer servers are located; probably, in recent years, more attention has been paid to IT security, and less attention to the fact that the physical security of the places is equally (if not more) important.

In addition, it is necessary to verify that the supplier has adopted a suitable recovery plan for the case of cyber-attacks or natural disasters that lead to connection problems, loss of data, etc.. For such cases, the Data Controller shall also carry out an assessment of the impact that loss of data or temporary impossibility of accessing them has on its activity and on the system's recovery time. In particular, companies offering essential continuous services that cannot afford prolonged inactivity shall pay attention to this aspect.

It is therefore necessary for the Data Controller to carefully assess the consequences on its organization of a possible interruption, of varying length, of the service offered, calculating the direct and indirect costs of data inaccessibility and defining in advance the emergency and recovery plan.

It is essential to adopt a suitable backup system that always allows access and recovery of data, even in the case of inaccessibility to the cloud system; it is therefore very important that the backup system is physically and informatically separated from the "main" system, so that it too cannot be affected by any problems suffered by the cloud. For example, in the case of the OVH fire, it seems that many customers were relying on the backup service provided by OVH itself, which for many is now also unusable, resulting in the futility of having such a backup system and continuing problems of data inaccessibility.

Data Controllers shall also pay a great deal of attention to the location of the cloud provider's servers, in particular whether the servers are located in the European Union or in non-EU countries (a problem that does not arise in the case of OVH, whose servers are located in Strasbourg, France). In fact, the GDPR (Articles 44 et seq.) allows the transfer of data to non-EU countries only if the adequacy of the non-EU country or organization is recognized by a decision of the European Commission (Article 45 of GDPR), or in the absence of such a decision, if the data controller or data processor provide(s) adequate safeguards including enforceable rights and effective remedies for data subjects (Article 46 of GDPR). And this should be particularly taken into account especially after the European Court of Justice on 16 July 2020 with the Schrems II judgment (C-311/18) annulled the European Commission Decision 2016/1250 which had affirmed the adequacy of the Privacy Shield (the EU-US shield regime).

Finally, very useful for the protection of the Data Controller (although obviously difficult to obtain in a normal contractual relationship between a small business and the cloud provider) are the contractual clauses providing for a right to compensation for damages or indemnification by the cloud provider or even penalty clauses for the case of incidents and malfunctions that result in data loss and may lead to sanctions and claims for damages by the data subjects.

Very useful, and to be positively assessed in the context of the choice of the cloud provider, is the presence of a suitable insurance policy that can cover any damages in the event of an accident.

Finally, it should not be forgotten that the Data Controller has, pursuant to Article 28, letter h) of GDPR, the right (which, however, also becomes a duty) to carry out inspections at the appointed External Data Processor, in order to verify the compliance with the obligations under the GDPR and the contract signed.

The brief remarks above, however, highlight the absolute centrality of the issues relating to the security of the cloud, the loss of data and the impossibility of recovering them as potentially implying a violation of the GDPR, with all the consequences of sanctions.

In fact, it should be recalled, in particular, that Article 32 of GDPR provides that both the Data Controller and the External Data Processor are required to implement "*appropriate technical and organizational measures to ensure a level of security appropriate to the risk*", always "*taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purposes of the processing, and also the risk of varying likelihood and severity for the rights and freedoms of natural persons*". More in detail, Art. 32 of GDPR, at letters b) and c), expressly provides that each of them shall guarantee the capacity to permanently ensure the integrity and availability of the data processing systems and services, as well as the capacity to "*promptly restore the availability and access of data in the event of a physical or technical incident*".

In conclusion, to return, for example, to the event that gave rise to this brief article, the fire in the OVH data centre could lead to the application of sanctions against both OVH and all companies, public and private, customers of OVH, if it emerges, at the outcome of the checks that will be conducted, a violation of security measures or an inability to restore timely availability and access to data.