OVH AND PERSONAL DATA PROTECTION

OVH
Innovation is Freedom

Founded in 1999, OVH is now one of the leading names in the cloud industry, with a presence in 19 countries across the world. We have more than 1 million customers, and we take utmost care to ensure that our customers' personal data is secure.

When you choose to host all or part of your data with OVH, you're entrusting us with a share of your digital assets. We're highly aware of the challenges this may pose for your organisation, particularly when it comes to compliance with data protection regulations. This is why we're providing you with as much information as possible regarding the challenges associated with personal data protection.

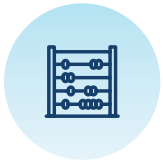
1 THE IMPORTANCE OF CHOOSING YOUR CLOUD SERVICES PROVIDER CAREFULLY

1.1. Compliance criteria

When you choose a cloud services provider, your decision shouldn't be based solely on technical challenges. Stricter regulations will soon be enforced by the EU 2016/679 General Data Protection Regulation (GDPR), and there is increasing public awareness of the ethical and economic challenges posed by the locations in which companies store their data. In response to this, leading cloud providers are adapting themselves accordingly, and looking beyond technological capacity. In addition to providing high-performance, secure services, OVH ensures that these solutions comply with all applicable data protection regulations, and maintains transparency in terms of how its solutions work.

These factors are crucial for any organisations that are looking to host their data with an external provider, since their compliance is fully dependent on the processor's. Because of our dedication to compliance, you can be sure that you are fully compliant with your own regulatory obligations. This requirement is stipulated in article 28 of the GDPR, which states that a "*controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation*[1]".

The French National Commission on Informatics and Liberty (CNIL), an authority whose mission is to ensure compliance with personal data protection laws, also advises that "*any [...] company planning to use a cloud computing service conducts a risk analysis and is very strict in the choice of its service provider. In particular, the company must take into consideration the guarantees offered by a service provider regarding the protection of personal data and must make sure that the service provider will give it all the necessary guarantees to fulfil its obligations under the Data Protection Act, particularly in terms of information to data subjects, regulation of transfers and data security*[2]".



1.2. Economic intelligence criteria

OVH is a pure player involved in a unique business: providing cloud-based IT infrastructures. Our business does not compete directly or indirectly (i.e. through other entities or subsidiaries) with our customers' businesses. This applies to both online sales and software publishing. Effectively, we consider it to be harmful when organisations inadvertently finance rival companies through their cloud providers, who justify this on the grounds that they are diversifying their business.

[1] Article 28 (EU) of the European Parliament and of the Council of 2016/679 April 27 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[2] CNIL, Recommendations for companies planning to use Cloud computing services: https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

2 OVH AND ITS COMMITMENTS AS A PROCESSOR OF PERSONAL DATA

OVH is classed as a "*processor*" when it processes personal data on behalf of a controller. This is typically the case when you store personal information on our infrastructures.

Commitment no.1: We do not re-use the data hosted on our services

OVH processes its customers' personal data solely for the purpose of fulfilling its services, and always follows the customer's instructions when doing so.

The data hosted within our services remains the property of the customer.

Any resale of the aforementioned data, as well as any use of the data for commercial purposes (e.g. profiling activity, or direct marketing), is strictly prohibited.

Commitment no.2: We offer data reversibility

"*Your data, your rules.*"

Data reversibility, i.e. the ability to migrate and repatriate your data in a standard format, is not offered with all cloud solutions on the market. At the very least, it can be made complicated by the existence of vendor lock-in policies. The cloud has become a strategic subject for companies. Too strategic to be worth taking risks on, or signing a lifelong contract with an operator. By advocating an open cloud, we can stop a few dominant players from setting the rules, just because they control part of the sector.

At OVH, all of our cloud solutions are based on open standards, including a number of open-source technologies. This way, you can recover and migrate your data easily, as your data is always reversible and interoperable.

Commitment no.3: You will always know exactly where your data is stored and processed

When you select a service that enables you to store your content and personal data, datacentre locations and geographical regions are always listed on our website. If several possible locations or geographical regions are available, you can choose a location when you place your order.

However, "*data storage*" is not a synonym for "*data processing*". The GDPR sets rules for "*processing*", not just for "storage". In light of this, it's good to take special care when you use these two terms.

When you select a storage region located in the EU, OVH guarantees that it will not process your data outside of the European Union, and any countries recognised by the European Commission as having a sufficient level of personal data protection regulations in place (with regard to the private lives, fundamental rights and freedoms of persons, and also with regard to exercising corresponding rights [adequacy decision]). We also guarantee that we will never process your data in the US.

Commitment no.4: We guarantee complete transparency in terms of recourse to subsidiaries as processors

OVH controls the entire hosting chain, from building its servers to managing its datacentres. With the exception of our subsidiaries, and unless otherwise stipulated in the specific terms and conditions of the service in question, no other company will be able to view or access our customers' data.

The full list of OVH subsidiaries is available on our website. Alternatively, customers can simply request it from our support teams. Our subsidiaries are just OVH's international offices: OVH Germany, OVH Spain, etc.

To ensure that our customers' data is optimally protected, OVH US is not considered to be a subsidiary. OVH US is completely separate from its European counterparts. We also notify our customers at least 30 days before any recourse to subsidiaries as processors.

Finally, if OVH ever needs to sub-contract an activity and this will involve viewing or accessing data, this operation will only be carried out with the customer's agreement.

Commitment no.5: We will inform you if your data privacy is breached

OVH maintains strict security measures. We also anticipate all scenarios, including data breaches.

If we ever experience a data breach, we will ensure that the customers concerned are informed as soon as possible. They will receive a notification describing the nature of the incident and its potential consequences, as well as the measures taken to resolve or minimise the breach.

Commitment no.6: We will provide comprehensive documentation for our services

It is essential that your cloud provider offers the appropriate guarantees for the critical nature of the data that will be processed. This is one of the criteria that will help you ensure that you are compliant with personal data protection regulations.

In order to make an appropriate decision and justify this to supervisory authorities, you need to have comprehensive documentation for all of the services offered by your processors. This is why OVH will provide you with all the appropriate documentation, including a description of the security measures put in place for your services, an attestation of the location your data is stored in, etc.

Commitment no.7: We will provide you with a contractual guarantee of our commitments

OVH commitments are not just idealistic promises: they're contractually integrated into our Data Processing Agreement (DPA). This document is provided as an attachment to our contracts. It is available on request to all of our customers.

3 OVH GUARANTEES REGARDING SECURITY

At OVH, we take every precaution to ensure that the personal data we process stays secure and confidential. More specifically, our objective is to stop it from being altered or accessed by non-authorised third parties.

3.1. Distribution of security actions to be implemented

It's important to address the difference between the security of the data hosted by the customer, and the security of the infrastructures on which this data is stored.

- Security of the data hosted: the customer is solely responsible for securing the resources and application systems they deploy as part of our services. OVH provides its customers with tools to help them secure their data.
- Infrastructure security: OVH ensures that its infrastructures are optimally secured. We have implemented an information systems security policy, and we meet the requirements for several standards and certifications: PCI DSS, ISO/IEC 27001 certification, SOC 1 type 2 and SOC 2 type 2 attestations, etc. We also have an accreditation for hosting healthcare data (HDS) as part of our Healthcare solution.

3.2. Security measures guaranteed by OVH

The security measures we guarantee depend on the services you use. We will provide you with the full, appropriate documentation for each solution. This helps our customers decide whether a solution has been suitably adapted to suit the personal data they would like to process.

For all of its services, OVH guarantees that it will put in place:

- Physical security measures to stop its infrastructures being accessed by non-authorised persons.
- Security personnel, responsible for ensuring that its datacentres remain physically secure, 24/7.
- A system for managing permissions, which will limit datacentre and data access to staff members who are required to access it as part of their role, and job scope.
- A physical and/or logical isolation system (depending on the service) for customers.
- A failsafe authentication process for users and admins, based on a strict password management policy, and the deployment of certain two-factor authentication measures, e.g. YubiKey.
- Processes and devices we can use to track all actions performed on our information system, and create reports on incidents that affect our customers' data, as per the regulations currently in effect.

WWW.OVH.COM