

DATA PROCESSING AGREEMENT

Version dated on May 25th, 2018

This Data Processing Agreement (“**DPA**”) forms part of the agreement, hereafter referred to as the “**Agreement**”, that is entered into between OVH Hosting Ltd. (“**OVH**”) and the Client, and that defines the terms and conditions applicable to the services performed by OVH (the “**Services**”). This DPA and the other provision of the Agreement are complementary. Nevertheless, in case of conflict, the DPA shall prevail.

Expressions which begin with an upper-case letter and which are not defined in this DPA shall have the meaning as set out in the Agreement.

The purpose of this DPA, which is entered into between OVH and the Client in accordance with article 28 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**General Data Protection Regulation**” or “**GDPR**”), is to define the conditions under which OVH is entitled, as a Processor and as part of the Services defined in the Agreement, to process under Client’s instruction, personal data as defined in the GDPR (“**Personal Data**”). The processing of personal data by OVH as a data controller is out of the scope of this DPA.

For the purpose of this DPA, OVH is acting as a “**Processor**” and the Client is presumed to act as a “**Controller**” provided that “Processor” and “Controller” have the meaning defined in the GDPR.

If the Client is acting as a processor on behalf of a third-party controller, the Parties expressly agree to the following conditions:

- (a) The Client shall ensure that (i) all the necessary authorisations to enter into this DPA, including the Client’s appointment of OVH as sub-processor, have been obtained from the Controller, (ii) an agreement, that is fully consistent with the terms and conditions of the Agreement including this DPA, has been entered into with the Controller pursuant to the said article 28 of the GDPR, (iii) any instructions received by OVH from the Client in execution of the Agreement and this DPA are fully consistent with the Controller’s instruction and (iv) all the information communicated or made available by OVH pursuant to this DPA is appropriately communicated to the Controller as necessary.
- (b) OVH shall (i) process Personal Data only under the Client’s instruction and (ii) not receive any instruction directly from the Controller, except in cases where the Client has factually disappeared or has ceased to exist in law without any successor entity taking on the rights and obligation of the Client.
- (c) The Client, which is fully responsible to OVH for the proper execution of the obligations of the Controller as provided under this DPA, shall indemnify and hold OVH harmless against (i) any failure of the Controller to comply with applicable law, and (ii) any action, claim or complaint from the Controller concerning the provisions of the Agreement (including this DPA) or any instruction received by OVH from the Client.



1. Scope

OVH is authorised, as a Processor acting under Client's instruction, to process the Controller's Personal Data to the extent necessary to provide the Services.

The nature of operations carried out by OVH on Personal Data may be computing, storage and/or any such other Services as described in the Agreement.

The type of Personal Data and the categories of data subjects are determined and controlled by the Client, at its sole discretion.

The processing activities are performed by OVH for the duration provided in the Agreement.

2. Selection of the Services

The Client is solely responsible for the selection of the Services. The Client shall ensure that the selected Services have the required characteristics and conditions to comply with the Controller's activities and processing purposes, as well as the type of Personal Data to be processed within the Services, including but not limited to when the Services are used for processing Personal Data that is subject to specific regulations or standards (as an example, health or banking data in some countries). The Client is informed that OVH proposes certain Services with organisational and security measures specifically designed for the processing of health care data or banking data.

If the Controller's processing is likely to result in high risk to the rights and freedom of natural persons, the Client shall select its Services carefully. When assessing the risk, the following criteria shall notably, but not limited to, be taken into account: evaluation or scoring of data subjects; automated-decision making with legal or similar significant effect; systematic monitoring of data subjects ; processing of sensitive data or data of a highly personal nature; processing on a large scale; matching or combining datasets; processing data concerning vulnerable data subjects; using innovative new technologies unrecognised by the public, for the processing.

OVH shall make available information to the Client, in the conditions set out below in clause "Audits", concerning the security measures implemented within the scope of the Services, to the extent necessary for assessing the compliance of these measures with the Controller's processing activities.

3. Compliance with Applicable Regulations

Each Party shall comply with the applicable data protection regulations including the General Data Protection Regulation from the date which it enters into force in the European Union.

4. OVH's obligations

OVH undertakes to:

- a) process the Personal Data uploaded, stored and used by the Client within the Services only as necessary to provide the Services as defined in the Agreement,
- b) neither access nor use the Personal data for any other purpose than as needed to carry out the Services (notably in relation to Incident management purposes),
- c) set up the technical and organisational measures described in the Agreement, to ensure the security of Personal Data within the Service,
- d) ensure that OVH's employees authorised to process Personal Data under the Agreement are subject to a confidentiality obligation and receive appropriate training concerning the protection of Personal Data,
- e) inform the Client, if, in its opinion and given the information at its disposal, a Client's instruction infringes the GDPR or other European Union or European Union Member State data protection provisions,
- f) in case of requests received from a competent authority and relating to Personal Data processed hereunder, to inform the Client (unless prohibited by the applicable laws or a competent authority's injunction), and to limit the communication of data to what the authority has expressly requested.

At the Client's written request, OVH will provide the Client with reasonable assistance in conducting data protection impact assessments and consultation with competent supervisory authority, if the Client is required to do so under the applicable data protection law, and in each case solely to the extent that such assistance is necessary and relates to the processing by OVH of Personal Data hereunder. Such assistance will consist of providing transparency about the security measures implemented by OVH for its Services.

OVH undertakes to set up the following technical and organisational security measures:

- (a) physical security measures intended to prevent access by unauthorised persons to the Infrastructure where the Client's data is stored,
- (b) identity and access checks using an authentication system as well as a password policy,
- (c) an access management system that limits access to the premises to those persons that need to access them in the course of their duties and within their scope of responsibility,
- (d) security personnel responsible for monitoring the physical security of the OVH premises,
- (e) a system that physically and logically isolates clients from each other,
- (f) user and administrator authentication processes, as well as measures to protect access to administration functions,
- (g) an access management system for support and maintenance operations that operates on the principles of least privilege and need-to-know, and
- (h) processes and measures to trace actions performed on its information system.

5. Personal Data Breaches

If OVH becomes aware of an incident impacting the Controller's Personal Data (such as unauthorised access, loss, disclosure or alteration of data), OVH shall notify the Client without undue delay.

The notification shall (i) describe the nature of the incident, (ii) describe the likely consequences of the incident, (iii) describe the measures taken or proposed to be taken by OVH in response to the incident and (iv) provide OVH's point of contact.

6. Location and transfer of Personal Data

In cases where the Services allow the Client to store content and notably Personal Data, the location(s) or, geographical area, of the available Datacenter(s) is specified on OVH Website. Should several locations or geographic areas be available, the Client shall select the one(s) of its choosing when submitting its Order. Subject to the applicable Special Terms of Service, OVH will not modify, without the Client's consent, the location or geographical area chosen when submitting its Order.

Subject to the foregoing Datacenters' location provision, OVH's Affiliates located within the European Union, Canada and any other country recognised by the European Union as providing an adequate level of protection for Personal Data ("**Adequacy Decision**"), excluding the United States of America, are allowed to process Personal Data only as needed for the carrying out of the Services, and in particular, in relation to Incident management purposes. The list of the Affiliates likely to take part in the carrying out of the Services is communicated as provided in the clause "Sub-processing" below.

The data stored by the Client within the scope of the Services shall not be accessed by OVH from a country which is not subject to an Adequacy Decision, unless (a) such access is expressly provided in the applicable Special Terms of Service, or (b) the Client selects a Data Center located outside the European Union in a country that is not subject to an Adequacy Decision or (c) Client's specific agreement.

In the event that Personal Data processed hereunder is transferred outside of the European Union to a country which is not subject to an Adequacy Decision, a data transfer agreement which complies with the Standard Contractual Clauses adopted by the European Commission, or at OVH's discretion, any other protection measures recognised as sufficient by the European Commission, shall be implemented. When such a transfer results from the selection by the Client of a Service for which a Data Center located outside European Union is used, the implementation of the aforesaid data transfer agreement (or equivalent measures of protection) is not automatic and shall require a specific Client's request.

The Controller shall complete all the formalities and obtain all necessary authorisation (including from data subjects and the competent data protection authorities, if required) to transfer Personal Data within the scope of the Agreement.

7. Sub-processing

Subject to the provisions of the clause “Location and transfer of Personal Data” above, OVH may engage another processor to process Personal Data as part of the performance of the Services (“**Sub-processor**”).

The Client expressly authorises OVH to engage Sub-processor Affiliates. The list of OVH Sub-processor Affiliates is available on OVH Website. OVH undertakes to give the Client thirty (30) days’ prior notice of any additional Sub-processor Affiliates.

Subject to any contradictory provisions of applicable Conditions of Service, OVH shall not engage non-Affiliate Sub-processors without the Client’s prior consent. When the applicable Conditions of Service provide the possibility to engage non-Affiliate Sub-processors, the validation of such Conditions of Service by the Client shall be considered as an approval of the relevant listed Sub-processors. The non-Affiliates Sub-processors are listed on OVH website or in the applicable Conditions of Service.

OVH shall ensure the Sub-processor is, as a minimum, able to meet the obligations undertaken by OVH in the present DPA regarding the processing of Personal Data carried out by the Sub-processor. For such purpose, OVH shall enter into an agreement with the Sub-processor. OVH shall remain fully liable to the Client for the performance of any such obligation that the Sub-processor fails to fulfil.

Notwithstanding the foregoing, OVH is expressly authorised to engage third-party providers (such as energy providers, network providers, network interconnection point managers or collocated datacenters, material and software providers, carriers, technical providers, security companies), without having to inform the Controller or obtain its prior approval, provided that such third-party providers do not access Personal Data.

8. Client’s and Controller’s Obligations

For the processing of Personal Data as provided under the Agreement, the Client shall provide to OVH in writing (a) any relevant instruction and (b) any information necessary to the creation of the Processor’s records of processing activities. The Client remains solely responsible for such processing information and instruction communicated to OVH.

The Controller is responsible to ensure that:

- a) the processing of Controller’s Personal Data as part of the execution of the Service has an appropriate legal basis (e.g., data subject’s consent, Controller’s consent, legitimate interests, authorisation from the relevant Supervisory Authority, etc.),
- b) any required procedure and formality (such as data protection impact assessment, notification and authorisation request to the competent data privacy authority or other competent body where required) has been performed,
- c) the data subjects are informed of the processing of their Personal Data in a concise, transparent, intelligible and easily accessible form, using clear and plain language as provided under the GDPR,

- d) data subjects are informed of and shall have at all the time the possibility to easily exercise their data rights as provided under the GDPR directly to the Client or to the Controller

The Client is responsible for the implementation of the appropriate technical and organisational measures to ensure the security of the resources, systems, applications and operations which are not in the OVH scope of responsibility as defined in the Agreement (notably any system and software deployed and run by the Client or the Users within the Services).

9. Data Subject Rights

The Controller is fully responsible for informing the data subjects of their rights, and to respect such rights, including the rights of access, rectification, deletion, limitation or portability.

OVH will provide reasonable cooperation and assistance, as may be reasonably required for the purpose of responding to data subjects' requests. Such reasonable cooperation and assistance may consist of (a) communicating to the Client any request received directly from the data subject and (b) to enable the Controller to design and deploy the technical and organisational measures necessary to answer to data subjects' requests. The Controller shall be solely responsible for responding to such requests.

The Client acknowledges and agrees that in the event such cooperation and assistance require significant resources on the part of the Processor, this effort will be chargeable upon prior notice to, and agreement with the Client.

10. Deletion and return of Personal Data

Upon expiry of a Service (notably in case of termination or non-renewal), OVH undertakes to delete in the conditions provided in the Agreement, all the Content (including information, data, files, systems, applications, websites, and other items) that is reproduced, stored, hosted or otherwise used by the Client within the scope of the Services, unless a request issued by a competent legal or judicial authority, or the applicable law of the European Union or of an European Union Member State, requires otherwise.

The Client is solely responsible for ensuring that the necessary operations (such as backup, transfer to a third-party solution, Snapshots, etc.) to the preservation of Personal Data are performed, notably before the termination or expiry of the Services, and before proceeding with any delete operations, updates or reinstallation of the Services.

In this respect, the Client is informed that the termination and expiry of a Service for any reason whatsoever (including but not limited to the non-renewal), as well as certain operations to update or reinstall the Services, may automatically result in the irreversible deletion of all Content (including information, data, files, systems, applications, websites, and other items) that is reproduced, stored, hosted or otherwise used by the Client within the scope of the Services, including any potential backup.

11. Liability

OVH can only be liable for damages caused by processing for which (i) it has not complied with the obligations of the GDPR specifically related to data processors or (ii) it has acted contrary to lawful written instructions of the Client. In such cases, the liability provision of the Agreement shall apply.

Where OVH and Client are involved in a processing under this Agreement that caused damage to data subject, the Client shall in a first time take in charge the full indemnification (or any other compensation) which is due to the data subject and, for second time, claim back from OVH the part of the data subject's compensation corresponding to OVH's part of responsibility for the damage, provided however that any limitation of liability provided under the Agreement shall apply.

12. Audits

OVH shall make available to the Client all the information necessary to (a) demonstrate compliance with the requirements of the GDPR and (b) enable audits to be carried out.

Such information is available in standard documentation on OVH Website. Additional information may be communicated to the Client upon request to OVH Support.

If a Service is certified, complies with a code of conduct or is subject to specific audit procedures, OVH makes the corresponding certificates and audit reports available to the Client upon written request.

If the aforesaid information, report and certificate prove to be insufficient to enable the Client to demonstrate that it meets the obligations laid down by the GDPR, OVH and the Client will then meet to agree on the operational, security and financial conditions of a technical onsite inspection. In all circumstances, the conditions of this inspection must not affect the security of others OVH's clients.

The aforementioned onsite inspection, as well as the communication of certificates and audit reports, may result in reasonable additional invoicing.

Any information that is communicated to the Client pursuant to this clause and that is not available on OVH Website shall be considered as OVH's confidential information under the Agreement. Before communicating such information, OVH may require to execute a specific non-disclosure agreement.

Notwithstanding the foregoing, the Client is authorised to answer to competent supervisory authority requests provided that any disclosure of information is strictly limited to what is requested by the said supervisory authority. In such a case, and unless prohibited by applicable law, the Client shall first consult with OVH regarding any such required disclosure.