Data Processing Agreement

This Data Processing Agreement ("**DPA**") is part of the Conditions of Services of the Services Agreement n° bj207337-ovh (the "**Agreement**") entered between OVH and DLSWest Stuttgart (the "**Client**"), hereafter referred to as the Parties.

The 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 into which OVH is entitled, as part of the Services delivered in execution of the Agreement, to process personal data under Client's instruction.

For the purpose of this DPA, OVH is acting as "Processor" and the Client is presumed to act as the "Controller" provided that *"Processor"* and *"Controller"* have the meaning defined in the GDPR.
If the Client is acting as a Processor, the Parties expressly agree on the following conditions:

(a) The Client shall ensure that (i) all the necessary authorizations to enter into this DPA has been obtained notably from the controller, (ii) an agreement, that is fully consistent with the terms and conditions of this DPA, has been entered into with the controller pursuant to the said article 28 of the GDPR, (iii) any instruction received by OVH from the Client in execution with the Agreement are fully consistent with controller's instruction and (iv), all the information communicated or made available by OVH and intended to the controller pursuant to this DPA are appropriately communicated to the controller.

(b) OVH shall (i) process the controller's data only under 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 against OVH for the proper execution of the obligations of the controller as provided under this DPA, shall warrant and hold OVH harmless against any failure of the controller to comply with its obligation provided under this DPA, as well as against any action, claim or complaint from the controller concerning any provision of this DPA or any instruction received by OVH from the Client in execution of the Agreement.

The processing of personal data by OVH as a Controller are out of the scope of this Appendix.

1. Compliance with Applicable Regulations

Each party shall comply with the applicable data protection regulations. OVH

particularly undertakes to comply with the regulation in force, at the location where the Services are provided, including any future applicable regulation, such as the General Data Protection Regulation, from the date which it enters in force in European Union.

2. Selection of the Services

The Controller is solely responsible for the selection of the Services. The Controller shall notably ensure that the selected Services have the required characteristics and conditions to comply with applicable laws and regulations notably taking into account the Controller's activities and processing purposes, as well as the type of the personal data to be processed within the Services, notably but not limited to when the Services are used for processing specifically regulated personal data (such as health or banking data).

The Processor undertakes to make available on the Processor Website, or on Controller's request to the Support, information concerning the security measures implemented within the scope of the Services, in order to allow the Controller to ensure that these measures correspond to its needs or those of its Data subjects or any third parties on whose behalf the Services are used.

Where such information is confidential, the Supplier may make it available to the Client only upon request, but may require the Client to first execute a non-disclosure agreement which is acceptable to OVH. The Processor may choose not to disclose some information deemed, in its sole discretion, high-sensitive security information.

In cases where the Services complies with a code of conduct, are certified or subject to specific audit procedures, the Processor can make the corresponding certificates and audit reports available to the Controller. Certification and audit reports communication may be subjected to additional fees.

When the Processor proposes Services specifically designed to host and/or process personal data subject to a specific regulation or standard, the Processor makes available to the Controller the Processor's scope of responsibility and the conditions into which the Processor complies with said standards or regulations.

3. Scope

Purpose of processing activities performed by OVH: supply and maintenance of infrastructures provided to the Client and containing Controller's Data.

Duration of the processing activities performed by OVH: period during which the Controller uses the Services as provided under the Agreement.

The Controller is responsible to ensure that the characteristics and conditions of the Services comply with the Controller's activities and processing purposes, as well as the type of personal data to be processed within the context of Services.

If the Controller's processing is likely to result in high risk to the rights and freedom of natural persons, the Controller 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 unrecognized by the public for the processing.

OVH is available to assist the Client in the relevant Data Protection Impact Assessment. In this respect, the Client is informed that OVH proposes Services with organizational and security measures specifically designed for the processing of health care data and banking data.

4. Obligations of the Controller

For the processing of Controller's data, the Client shall provide any relevant instruction to the Processor in writing and remains solely responsible for such data instruction.
The Client represents and warrants that:

a) it has an appropriate legal basis (e.g., Data Subject's consent, Controller consent, legitimate interests, authorization from the relevant Supervisory Authority, etc.) to process and disclose the Controller Personal Data to the Processor as part of the provision of the Service,
b) it has performed any required procedures and formalities (such as Data Protection Impact assessment, notification and authorization request to the competent data privacy authority or other competent body) and obtain all the necessary authorization,
c) it took appropriate measures to provide any mandatory information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language,
d) it informed data subject that any data rights must be exercised directly with the Client or the Controller and not with the Processor,
e) it has reviewed the information made available by the Processor including operational, technical and organizational measures,
f) it will provide to the Processor any information necessary to the creation of the Processor's records of processing activities.

The Controller is responsible for ensuring the security of resources, systems and applications which it deploys within the scope of the use of the Services, and, in particular, is responsible for setting up data filtering systems such as firewalls, update deployed systems and software, manage access rights, configure resources, etc. The Processor shall in no way be responsible for security incidents linked to the use of the Internet, in particular (but not limited to) in case of loss, alteration, destruction, disclosure or unauthorized access to the Client's data or information.

5. Obligations of the Processor

When processing the data uploaded, stored and used by the Client within the Services, OVH is acting as Processor under the Controller's instruction as provided under the Agreement, or in writing by the Client.

The Processor undertakes to:

a) process the Personal Data uploaded, stored and used by the Client within the Services only as necessary to provide the Services, subject to the Data Controller's written instructions,
b) neither access nor use the Controller's data for any purposes other than as needed to carry out the Services (and, in particular, in relation to Incident management purposes), and notably not process any Controller Personal Data for the purposes of data mining, profiling or direct marketing activities as defined in the General Data Protection Regulation,
c) set up the organizational and security measures described in this article to ensure the confidentiality and integrity of the personal data controlled and used by the Client within the Service, and particularly to prevent unauthorized or unlawful processing, accidental loss or destruction of or damage to such data,
d) ensure that Processor's employees authorized to process personal data under the Agreement are subject to a confidentiality obligation and receive a necessary appropriate training concerning the protection of personal data,
e) inform the Controller, if in its opinion and given the information at its disposal, a Controller's instruction infringes the GDPR or other Union or Member State data protection provisions.
f) in case of request received from a competent judicial or legal authority and relating to Controller's data, the Processor undertakes to inform the Controller, unless prohibited by applicable law or authority's injunction, and to limit the communication of data to what the authority has expressly requested,
g) comply with any other obligation provided under this DPA.

The Processor undertakes to establish:

(a) physical security measures intended to prevent access by unauthorized persons to the Infrastructure where the Client data is stored,
(b) identity and access checks using an authentication system as well as a password policy,
(c) an access management system which limits access to the premises to those persons which 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 Supplier 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 all actions performed on its information system.

6. Location and Transfer of Data

In cases where the Services allow the Client to store Content and notably personal data, the location(s) or, geographic 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, the Processor forbid itself to modify, without the Client's consent, the location or geographic area chosen when submitting its Order.

Subject to the previous provision related to the Datacenters' location, the Processor Affiliates within the European Union, Canada and any other country recognized 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 the data hosted by the Client within the scope of the Services and only as needed for the carrying out of said 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 article "Sub processing" below.

The data stored by the Client within the scope of the Services shall not be accessed by the Processor 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 which is not subject to an Adequacy Decision or (c) Client's specific agreement.

In the event that Controller's personal data is transferred outside of the European Union in 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 the Processor discretion, any other protection measures recognized as sufficient by the European Commission, may 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 authorization notably from the person concerned and the competent data protection authorities to transfer its personal data in the scope of the Services Agreement.

7. Sub processing

Subject to the provisions of the article “Localization and Data Transfer” above, the Controller acknowledges and expressly authorizes the Processor to engage Affiliates to sub process Controller’s data as part of the performance of the Services.

The list of such Affiliates is available on OVH website or upon request to OVH Support. The Processor undertakes to communicate thirty (30) days in advance any additional sub processor Affiliates.

Subject to any contradictory provisions of applicable Specific Terms of Service, the Processor shall not engage non-Affiliates sub processor without Controller’s prior consent.

The Processor shall ensure the sub processor is as a minimum able to meet the obligations undertaken by the Processor in the present DPA regarding the processing of personal data carried out by the sub-processor.

At the Controller’s request, the Processor provides the Controller with reasonable information concerning the actions and measures the Processor and its sub-processors have undertaken to practically comply with the provisions set forth in this DPA.

If the Controller objects to a sub-processor, the Controller may immediately terminate the Services or, if agreed by the Controller and Processor, only the part of the Service which is performed by the sub-processor.

OVH is expressly authorized to freely recourse to third-party providers (such as energy providers, network providers, network interconnection point managers or collocated datacenters, material and software providers, carriers, technical providers, security company), without having to inform the Controller or obtain its prior approval, provided that such third-party providers do not access Controller’s data.

8. Audits

In addition to the information available to the Controller as provided under Article II above, when the Services are certified or subject to specific audit procedures, the Processor can make the corresponding certificates and audit reports available to the Controller.

Certain Services are eligible for On-Site audits under the conditions provided for in the applicable Special Terms of Service.

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

9. Liability

The Processor can only be liable for the damage caused by processing only where (i) it has not complied with obligations of the GDPR specifically directed to processors or where (ii) it has acted contrary to lawful written instructions of the Controller.

Where the Controller and the Processor are involved in the same processing and where they each have a part of responsibility for any damage caused by processing, the Controller will in a first time compensate the entire damage to the data subject. The Controller can, in a second time, claim back to the Processor the part of the compensation corresponding to its part of responsibility for the damage, provided that any limitation of liability under the Agreement shall apply.

10. Data Subject Rights

The Controller is fully responsible to inform the Data Subjects of their rights, and to respect such rights, including the rights of access, rectification, deletion, limitation, portability or deletion.

The Processor will provide the Controller with reasonable co-operation and assistance, as may be reasonably required for the purpose of responding to Data Subjects. Such reasonable co-operation and assistance may consist in (a) communicating to the Controller any request received directly from the Data Subject and (b) to enable the Controller to design and deploy the technical and organizational measures necessary to answer to Data Subjects' requests.

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

11. Security Breach

If the Processor becomes aware of a security incident impacting the Controller's personal data (such as unauthorized access, loss, disclosure or alteration of data), the Processor shall notify the Client without undue delay.

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

12. Deletion and return of Personal Data

The Processor shall not technically restrict the Controller's ability to retrieve and delete its data.

Notwithstanding the foregoing, the Controller is solely responsible to perform any operations (such as backup, transfer to a third-party solution, Snapshots, etc.) which are necessary to the preservation of Controller's data, notably before the termination or expiry of the Services, and before proceeding with any delete operations, update or reinstallation of Services.

In this respect, the Controller is informed that the termination of Services for any reason whatsoever (in particular, the termination or non-renewal of the Agreement, failure to comply with the Terms of Service, etc.), as well as certain operations to update or reinstall the Services, shall automatically result in the irreversible deletion of all Content (including information, data, files, systems, applications, websites, and other items) that is reproduced, stored, hosted, collected, transmitted, distributed, published and more generally used and/or operated by the Client within the scope of the Services, including any potential backup.