DATA PROCESSING AGREEMENT

Version dated on 26.02.2020

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. "Binding Corporate Rules", "Controller", "Personal Data", "Personal Data Breach", "Processing", "Processor", "Supervisory Authority" are interpreted as defined in 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**").

Part 1 – Personal Data Processed by OVH as a Processor under Client's instruction

The purpose of this part is to define, according to article 28 of the GDPR, the conditions under which OVH is entitled, as a Processor and as part of the Services defined in the Agreement, to carry out the processing of Personal Data on behalf of, and on instructions from the Client.

For the purpose of this part, the Client may act either as **"Controller" or "Processor"** with respect to Personal Data. 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 section "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 regulation (including the General Data Protection Regulation).

4. OVH's obligations

OVH undertakes to:

a) process the Personal Data uploaded, stored and used by the Client within the Services only to the extent necessary and proportionate 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 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.

These technical and organizational measures are further detailed on OVH Website.

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 any contrary provision of 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.

The Personal Data stored by the Client shall not be transferred by OVH to a country which is not recognised by the European Commission as providing an adequate level of protection ("Adequacy Decision"), unless (a) such transfer is expressly provided for in the applicable Terms and Conditions, or (b) the Client selects a Datacenter located outside the European Union in a country that is not subject to an Adequacy Decision or (c) with Client's consent.

Subject to the foregoing Datacenters' location provision, OVH and authorized Sub-Processors' pursuant to section 7 below may, except from the United-states of America, remotely process Client's Content provided that such access shall occur only as needed for the carrying out of the Services, and in particular, in relation to security and Incident management purposes.

If, pursuant to the Agreement, Personal Data processed hereunder is transferred outside of the European Union to a country which is not subject to an Adequacy Decision, or accessed from such a non-European country, a data transfer agreement which complies with the Standard Contractual Clauses adopted by Decision n°2010/87/EU dated 5 February 2010 of the European Commission, or at OVH's discretion, any other appropriate safeguards pursuant to Chapter V "Transfers of personal data to third countries or international organisations" of the GDPR, shall be implemented. The Client hereby grants OVH power of attorney to enter into the aforesaid Standard Contractual Clauses with the Data Importer, in the name of and on behalf of the Data Exporter, and represents and warrants to have all the necessary authorization.

When Standard Contractual Clauses are implemented, the following shall apply:

(a) For clauses 5 f) and 12 (2) of the Standard Contractual Clauses, the provisions of the section 12 of this DPA apply.
(b) For clause 11 of the Standard Contractual Clauses, the Client consents OVH and the Data Importer to engage sub-processors in the conditions provided in section 7 of this DPA.
(c) For clause 12 (1) of the Standard Contractual Clauses, the Data Importer shall, in the conditions provided under the Agreement, and notably the section 10 "Deletion and return of Personal Data" of this DPA, (i) assist the Data Exporter to get back its data and (ii) delete the Data Exporter's data.
(d) If the Data Importer is held liable for a violation of its obligation under the Standard Contractual Clauses, any liability provision of the Agreement, notably but not limited to the section 11 of this DPA, shall apply to and be fully binding and enforceable against the Data Importer and Data Exporter.

The purpose of the previous paragraph is to specify how the Parties agree to apply the Standard Contractual Clauses, and not to derogate to or conflict with the Standard Contractual Clauses. In case of conflict the Standard Contractual Clauses shall have precedence.

The Controller shall complete any assessment (such as privacy impact assessment) and obtain all necessary authorisation (including from data subjects or 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 section "Location and transfer of Personal Data" above, OVH is authorized to engage sub-contractors to assist it in providing the Services. As part of such assistance, the sub-contractors may participate in the data processing activities performed by OVH under the Client's instruction.

The list of sub-contractors which are authorized to take part in the processing activities performed by OVH under the Client's instruction ("**Sub-processor(s)**"), including the Services concerned and the location from which they may process Client's Personal Data according to this Agreement, is provided (a) on OVH Website or, (b) when a Sub-Processor takes part only to a specific Service, in the relevant applicable Specific Terms and Conditions.

If OVH decides to change a Sub-processor or to add a new Sub-processor ("**Sub-processor Change**"), OVH shall notify the Client by email (to the email address registered in the Client Account) (a) thirty (30) days in advance if the Sub-Processor is an OVH Affiliate located in the European Union or in a country that is subject to an Adequacy Decision, or (b) ninety (90) days in advance in any other case. The Client has the right to object to a Sub-Processor Change as provided under GDPR. The objection shall be notified to OVH within fifteen (15) days following the Sub-processor Change notice by OVH to the Client and specifying the reason for the objection. Such objection shall be notified by the Client through its Management Interface using the category "Data Protection request" or in writing to *Data protection Officer, OVH SAS, 2 rue Kellermann 59100 Roubaix (France)*. OVH shall in no case be obliged to renounce to a Sub-processor Change. If following a Client's objection, OVH does not renounce to the Sub-Processor Change, the Client has the right to terminate the Services affected.

OVH shall ensure any 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.

OVH is hereby 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), wherever they are located, without having to inform the Client nor obtain its prior approval, to the extent such third-party providers do not process the Client's Personal Data.

8. Client'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 for 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 Client is responsible to ensure that:

a) the processing of 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 rights as provided under the GDPR directly 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 section and that is not available on OVH Website shall be considered as OVH's confidential information under the Agreement. Before communicating such information, the Client may be required 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.

13. Contact OVH

For any question concerning personal data (incident, conditions of use, etc.), the Client can contact OVH as follow:

(a) Creation of a ticket in its Client Account Management Interface,

(b) Use of the contact form provided for this purpose on the OVH Website,

(c) By contacting its OVH Support Service,

(d) By post to the address: OVH SAS, Data Protection Officer, 2 rue Kellermann, 59100 Roubaix.

Part 2 – Personal Data Processed by OVH as a Controller

The purpose of this Part is to define the conditions under which OVH processes Personal Data as a Controller.

1. Purpose of the Data processing

As part of the implementation of the Agreement, personal data relating to the Client and to the use of the Services are processed by OVH acting as Controller, in order to (a) manage its customer relationship (management of commercial activities, Client information and support, claims, invoicing, accountancy, payment management, debt collection, improvement of the ordering process, loyalty program, etc.), (b) Services delivery (delivery, maintenance, development and management of the quality and the security of the Services, etc.), (c) prevent fraud, payment default and utilisation of the Services which does not comply with the regulation or with the applicable Terms and Conditions of Service, (d) comply with applicable laws and regulations (obligation to archive and retain data such as connexion logs and user identification) and (e) enforce its rights.

2. Type of Data

The Personal Data processed by OVH are (i) personal data relating to the Client (first name, last name, postal address, email address, phone numbers, identification number or "NIC Handle", etc.), (ii) interaction between the Client and OVH (support contacts, exchanges, minutes, etc.), (iii) accounting and financial information (order history, invoices, credit note, payment means including owner of the payment, etc.), (iv) technical information concerning the utilization of services (connection ID, services ID, connection logs, use of the Services history, etc.).

Such processing activities are performed in compliance with applicable law, especially the GDPR.

3. Conditions of processing

OVH Affiliates participate to the aforementioned processing activities and OVH relies on third-party providers such as security services, payment services, network services and other service providers (mailing, survey, carriers, marketing analysis, analysis of OVH Group website activities, etc.) acting as processors under OVH's instructions (the "Processor(s)"). In such cases, an agreement which complies with applicable law, is entered into between the Processor and OVH, and appropriate technical and organisational measures are implemented according to articles 28 and 32 of the GDPR.

If Personal Data is transferred (including by a remote access) outside of the European Union to a country that is not subject to an Adequacy Decision, appropriate safeguards are provided pursuant to Chapter V of the GDPR such as (at OVH discretion) a data transfer agreement which complies with the standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) or adopted by the European Commission in accordance with the examination procedure referred to in the same article, or binding corporate rules or any other protection measures recognized as ensuring an adequate level of protection by the European Commission.

The conditions of aforesaid Personal Data processing are detailed on OVH website. OVH reserves the right to update such conditions from time to time and communicates on the relevant changes.

OVH undertakes not to use the aforesaid Personal Data for any purpose that is not compatible with the aforementioned purposes, provided however that OVH may be required to communicate the said Personal Data in response to a request or decision of authorities (such as judicial and/or administrative authorities). In that case, OVH undertakes to inform the Client (unless prohibited by applicable law or by the authority), and to communicate only Personal Data that are required.

Notwithstanding the foregoing, OVH reserves the right to anonymize the Data subject of this part. Such anonymized data may be retained, processed and used in such anonymized format for any purpose (notably to produce statistics, develop and improve services, perform marketing analysis, develop businesses, etc.).

4. Data Subject rights

According to the GDPR, the Client can lodge a complaint with the competent supervisory authority, and exercise its right of access, rectification, erasure, limitation, portability and opposition to aforementioned personal data which concerns it.

The Client may exercise this right and obtain said information from OVH by using the dedicated form on the OVH Website or by post at the address: OVH, Data Protection Officer, 2 rue Kellermann, 59100 Roubaix, France. Any such requests must include proof of identity. All such requests shall be answered within thirty (30) days of receipt.