DATA PROCESSING AGREEMENT

Version dated on 27.09.2021

This Data Processing Agreement ("**DPA**") forms part of the agreement, hereafter referred to as the "**Agreement**", that is entered into between OVH Hosting Ltd. ("**OVHcloud**") and the Client, and that defines the terms and conditions applicable to the services performed by OVHcloud (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. "Data Subject", "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**").

The purpose of this DPA is to define, according to article 28 of the GDPR, the conditions under which OVHcloud 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, excluding the personal data processing activities performed by OVHcloud as a controller. The conditions into which OVHcloud processes, as a Controller, Personal Data relating to the Client (including the Client's agents), are defined in the OVHcloud Data Usage Policy.

For the purpose of this DPA, 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 OVHcloud 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 OVHcloud 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 OVHcloud pursuant to this DPA is appropriately communicated to the Controller as necessary;

(b) OVHcloud 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 OVHcloud for the proper execution of the obligations of the Controller as provided under this DPA, shall indemnify and hold OVHcloud 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 OVHcloud from the Client.

1. Scope

1.1 OVHcloud 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.

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

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

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

2. Selection of the Services

2.1 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 OVHcloud proposes certain Services with organisational and security measures specifically designed for the processing of health care data or banking data.

2.2 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.

2.3 OVHcloud 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. OVHcloud's obligations

4.1 OVHcloud 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 OVHcloud'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.

4.2 In case of requests received from judicial, administrative or other authorities to obtain communication of Personal Data processed by OVHcloud pursuant to this DPA, OVHcloud makes reasonable efforts to (i) analyse the competence of the requesting authority and the validity of the request, (ii) respond only to authorities and requests that are not obviously incompetent and invalid, (iii) limit the communication to data required by the authority and (iv) beforehand inform the Client (unless prohibited by applicable law).

4.3 If the request is coming from a non-European authority in order to obtain communication of personal data processed by OVHcloud pursuant to this DPA on behalf of an European Client, OVHcloud objects to the request, subject to the following cases:

(x) the request is made in accordance with an international agreement, such as a mutual legal assistance treaty, in force between the requesting country and the European Union or the Member State where the personal data is located or the Member State of the OVHcloud entity to which the customer registered its OVHcloud customer account;
(y) the requested Personal Data is stored in a data center located outside the European Union;
(z) the request is made in accordance with Article 49 of the GDPR, particularly pursues an important reason of public interest recognised by Union or Member State law of the European Union, or is necessary to safeguard vital interests of the data subject or of other persons.

4.4 At the Client's written request, OVHcloud 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 OVHcloud of Personal Data hereunder. Such assistance will consist of providing transparency about the security measures implemented by OVHcloud for its Services.

4.5 OVHcloud 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 OVHcloud 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.

4.6 These technical and organisational measures are further detailed on OVHcloud Website.

5. Personal Data Breaches

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

5.2 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 OVHcloud in response to the incident and (iv) provide OVHcloud's point of contact.

6. Location and transfer of Personal Data

6.1 When a Service allows the Client to store Content and notably Personal Data, the location(s) or, geographical area, of the available Datacenter(s) is specified on OVHcloud 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, OVHcloud does not modify, without the Client's prior approval, the location or geographical area chosen when submitting its Order.

6.2 Subject to the foregoing Datacenters' location provision, OVHcloud and authorised Sub-Processors pursuant to section 7 below, may remotely process Client's Content provided that such processing operations occur as needed for the carrying out of the Services, and in particular, in relation to security and service maintenance purposes.

6.3 Concerning the utilisation of Services located in non-European Datacenters, (a) the Datacenters may be located in countries which are not subjected to an adequacy decision of European Commission pursuant to article 45 of the GDPR ("Adequacy Decision") and/or (b) the Client's Content may, according to sections 6.2 and 7 of this DPA, be processed from countries not subjected to an Adequacy Decision.

6.4 If for the purpose of Personal Data processing subjected to the GDPR, the Client intends to use Services referred to in the section 6.3 above, the standard data protection clauses adopted by the Commission implementing decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "Standard Contractual Clauses"), shall be implemented beforehand. To this end, the Client shall contact OVHcloud, provided that OVHcloud gives no guarantee concerning the implementation feasibility and the effectiveness of the Standard Contractual Clauses.

6.5 Concerning Services located in European Datacenters, if the applicable terms and conditions provide that the Personal Data processing subject to this DPA may be operated from one or several non-European countries which are not subjected to an Adequacy Decision, OVHcloud makes available Standard Contractual Clauses which shall apply to the transfers, or, at OVHcloud discretion, implements any other appropriate safeguards pursuant to Chapter V of the GDPR.

6.6 In case of Standard Contractual Clauses implementation according to the sections 6.3, 6.4 and 6.5 of this DPA, the Client is responsible to (i) assess the effectiveness of the Standard Contractual Clauses (including the relevant technical and organizational measures), taking into account notably the

categories of data that the Client intends to process as part of the Services, and the laws and practices of the receiving countries, in order to establish if there is anything in the said law or practices that may impinge on the effectiveness of the Standard Contractual Clauses, and (ii) if the assessment reveals that the Standard Contractual Clauses are not effective, implement, as recommended by the European Data Protection Board, any supplementary measure to ensure a level of protection essentially equivalent to that guaranteed within the European Union. OVHcloud undertakes to assist the Client by communicating, upon request, any information in his possession that may be useful for the Client's assessment.

6.7 Any applicable Standard Contractual Clauses shall be supplemented by the other applicable Conditions of Services (including this DPA) which apply *mutatis mutandis* to both the Data Importer(s) and Data Exporter(s), provided that they do not conflict with the Standard Contractual Clauses. In case of conflict the Standard Contractual Clauses shall have precedence.

7. Sub-processing

7.1 Subject to the provisions of the section "Location and transfer of Personal Data" above, OVHcloud is authorised 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 OVHcloud under the Client's instruction.

7.2 The list of sub-contractors which are authorised to take part in the processing activities performed by OVHcloud 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 OVHcloud Website or, (b) when a Sub-Processor takes part only to a specific Service, in the relevant applicable Specific Terms and Conditions.

7.3 If OVHcloud decides to change a Sub-processor or to add a new Sub-processor ("**Sub-processor Change**"), OVHcloud shall notify the Client in its control panel or by email (to the email address registered in the Client Account) (a) thirty (30) days in advance if the Sub-Processor is an OVHcloud 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 OVHcloud within fifteen (15) days following the Sub-processor Change notice by OVHcloud 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)*. OVHcloud shall in no case be obliged to renounce to a Sub-processor Change. If following a Client's objection, OVHcloud does not renounce to the Sub-Processor Change, the Client has the right to terminate the Services affected.

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

7.5 OVHcloud 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

8.1 For the processing of Personal Data as provided under the Agreement, the Client shall provide to OVHcloud 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 OVHcloud.

8.2 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

8.3 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 OVHcloud 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

9.1 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.

9.2 OVHcloud 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.

9.3 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

10.1 Upon expiry of a Service (notably in case of termination or non-renewal), OVHcloud 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.

10.2 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.

10.3 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

11.1 OVHcloud 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.

11.2 Where OVHcloud 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 OVHcloud the part of the Data Subject's compensation corresponding to OVHcloud's part of responsibility for the damage, provided however that any limitation of liability provided under the Agreement shall apply.

12. Audits

12.1 OVHcloud 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 OVHcloud Website. Additional information may be communicated to the Client upon request to OVHcloud Support.

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

12.3 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, OVHcloud 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 OVHcloud's clients.

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

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

12.6 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 OVHcloud regarding any such required disclosure.

13. Contact OVHcloud

For any question concerning personal data (incident, conditions of use, etc.), the Client can contact OVHcloud 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 OVHcloud Website,

(c) By contacting its OVHcloud Support Service,

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