DATA PROCESSING AGREEMENT

Version dated on 2023/03/24

This Data Processing Agreement ("**DPA**") forms part of the agreement, hereafter referred to as the "**Agreement**", that is entered into between OVH India. ("**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.

The terms "**Data**" and "**Information**" shall have the meaning ascribed to them under the Information Technology Act, 2000. The term "**Personal Data**" shall have the meaning ascribed to the term "**Personal Information**" under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("**Privacy Rules**"). Reference to "Sensitive Personal Data or Information" shall borrow its meaning from Rule 3 of the Privacy Rules. The term "Personal Data" for the purposes of this Agreement shall include "Sensitive Personal Data or Information". The term "Controller" means a person who, alone or jointly with others, determines the purposes and means of the processing of Personal Data of the Data Subject. "Data Subject" means any person whose Personal Data is protected under the applicable provisions of the Privacy Rules.

The purpose of this DPA is to define the conditions under which OVHcloud is entitled, as part of the Services defined in the Agreement, to carry out, on behalf of and on instructions from the Client, the processing of any Personal Data that is hosted by the Client within the Services, excluding any Personal Data defined in the OVHcloud Data Privacy Policy that is processed by OVHcloud for its own account.

1. Scope

1.1 OVHcloud is authorised, as a data processor acting under Client's instruction, to process the Controller's Personal Data ("**Processor**") 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).

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; automateddecision 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 Information Technology Act, 2000 and the rules framed thereunder).

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 applicable laws.

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 may 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

4.3 If the request is coming from a nonIndian authority in order to obtain communication of personal data processed by OVHcloud pursuant to this DPA, 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 India or the country where the personal data is located or where the OVHcloud entity to which the customer registered its OVHcloud customer account is located;
(y) the requested Personal Data is stored in a data center located outside India;
(z) the request pursues an important reason of public interest recognised by India, or is necessary to safeguard vital interests of the data subject or of other persons.

4.4 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.

4.5 These technical and organisational measures are further detailed on https://www.ovhcloud.com/india/en-in/personal-data-protection/security/ provided for this purpose on the OVHcloud Website,

5. **Contact OVHcloud**

For any question concerning Personal Data, the Client can contact OVHcloud as follow:

(a) By contacting its OVHcloud Support Service,
(b) By post to the address: OVH WeWork Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076, India.