DATA PROCESSING AGREEMENT

Version dated on 23.01.2023

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.

OVHcloud

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 In the event that the Customer uses the Services referred to in the paragraph above for the purpose of processing personal Data subject to the GDPR, the Customer is considered as the Data Controller, OVHcloud as its processors and OVHcloud subsidiaries as sub-processors. When personal data is transferred to subsidiaries in countries that do not have an Adequacy Decision, OVHcloud is considered a Data Exporter and its subsidiaries a Data Importer under the GDPR. In this context, OVHcloud and its subsidiaries have concluded standard contractual clauses adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (hereinafter "Standard Contract Clauses"), annexed to this DPA and intended to apply to the aforementioned transfers.

6.5 For Services located in datacenters located within the European Union, if the applicable Conditions of Service provide that the processing of the Personal Data subject to this DPA may be

carried out from one or more countries not benefiting from an Adequacy Decision, the Types of Contractual Clauses mentioned above apply.

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. Furthermore, the Customer remains responsible for completing any formality and/or obtaining any authorisation or consent that may, where appropriate, be required to enable the transfer of personal data to countries that do not have an Adequacy Decision.

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.

STANDARD CONTRACTUAL CLAUSES

Transfers from processor to processor [Module 3]

PREAMBLE

OVH SAS is the (direct or indirect) parent company of the OVH European Affiliates.

OVH SAS and the OVH European Affiliates are selling services, including without limitation infrastructure as a service and cloud services (together the "**Services**").

As part of their activities and notably the execution of the Services, OVH SAS and the OVH European Affiliates are processing personal data subjected to 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 (the "**GDPR**"), notably personal data of their Clients.

Such personal data processing activities are performed by OVH SAS and the OVH European Affiliates either (a) as controller or (b) as a processor under their Clients' instructions.

OVH SAS and the OVH European Affiliates, at the express request of their Clients, may transfer the aforementioned processing activities to one or more data importers located in a country which is not considered by the European Commission as a third country that ensures an adequate level of protection according to article 45 of the GDPR. Such processing activities will be performed by the relevant data importer as a processor under instruction of the relevant data exporter. The performance of such processing activities implies a transfer of personal data to the data importer (including remote access from its country).

The data importer's country is not considered by the European Commission as a third country that ensures an adequate level of protection according to article 45 of the GDPR.

For the purposes of Articles 28 (7) and 46 (c) of the Regulation (EU) 2016/679,, the parties have agreed on the following Contractual Clauses adopted by Decision n°2021/914/EU dated 4 June 2021 of the European Commission, which integrates the clauses of Module 3 applicable to transfers from processor to processor (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

The following Clauses are only applicable to personal data processing activities performed by OVH SAS and the OVH European Affiliates as processor under their Clients' instructions entrusted to the relevant data importer as a processor.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the legal persons (hereinafter 'entities') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entities in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfers

The details of the transfers, and in particular the categories of personal data that are transferred and the purposes for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout

the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the

purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant

certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)

The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in

the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual

residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Parties for any damages it causes the other Parties by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to

the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the

controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU)

2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) THE PARTIES AGREE THAT THOSE SHALL BE THE COURTS OF FRANCE.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

Capitalized terms shall have the meaning set forth in the agreement concluded between OVH Cloud Hosting Ltd and its Clients, which includes the Data Processing Agreement, the Privacy Policy and all other documents parts of the agreement.

ANNEX I

A. LIST OF PARTIES

Data exporter (processor)

OVH SAS

Company incorporated under French Law whose registered office is located at 2 rue Kellermann 59100 Roubaix (France),

OVH Hispano

Company incorporated under Spanish law whose registered office is located C/ Alcalá 21, 5° planta, 28014 Madrid (Spain),

OVH SRL

Company incorporated under Italian law whose registered office is located Calle San Lucas B. Roca y Coronado n° 3 zona: sur santa cruz, Bolivia (Italy),

OVH GmbH

Company incorporated under German law whose registered office is located Christophstraße 19, 50670 Köln (Germany),

OVH Hosting Limited

Company incorporated under Irish law whose registered office is located Enterprise House, O'Brien road, Carlow, R93Y0Y3 (Ireland),

OVH Sp. Zo.o.

Company incorporated under Polish law whose registered office is located ul. Szkocka 5/1 54-402 Wrocław (Poland),

OVH Hosting Sistemas informaticos unipessoal

Company incorporated under Portuguese law whose registered office is located Avenida Miguel Bombarda, 133 6aA 1050-164 Lisboa (Portugal),

OVH BV

Company incorporated under Dutch law whose registered office is located Hogehilweg 16, Amsterdam, 1101CD (Netherlands),

OVH SAS and OVH European Affiliates contact point for standard contractual clauses :

OVH - Data Protection Officer - 2 rue Kellerman 59100 Roubaix

Activities relevant to the data transferred under these Clauses:

Computing, storage and/or any such other Services as described in the agreement concluded with the Clients.

Data importer (processor)

OVH Singapore PTE Ltd, Company incorporated under Singaporean law whose registered office is located 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore). Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	**Altimat Data Center Singapore PTE. Ltd,** Company incorporated under Singaporean law whose registered office is located 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore) Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
OVH Australia PTY Ltd, Company incorporated under Australian law whose registered office is located north Sydney, 2060, New South Wales (Australia), registered under company number 612612754.	**Data Center Sydney PTY Ltd,** Company incorporated under Australian law whose registered office is located north Sydney, 2060, New South Wales (Australia).

Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**
Contact point for Singapore and Australia entities: **OVH Singapore PTE Ltd,** 135 Cecil street #10-01, Philippine airlines building, 069536 (Singapore).	
OVH Tech R&D Private Limited, Company incorporated under Indian law, whose registered office is located at Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India Contact point: Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**	**Altimat Data Center India Private Limited,** Company incorporated under Indian law, whose registered office is located at H No. 215, A102 1st Floor A Wing, Narpoli, Golden Park, Rallway Stn Road, Anjur Phata, Bhiwandi, Thana, Maharashtra, India, 421302 Contact point: Salapuria Symbiosis, Areke Village, Begur Hobli, Bannerghatta Road, Bengaluru, Karnataka, 560076 India Activities relevant to the data transferred under these Clauses: **Computing, storage and/or any such other Services (i) hosted in Datacenter(s) located in Asia-Pacific area or (ii) for which the applicable Specific Terms and Conditions provide these OVH Affiliates may participate to carry out such Services**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The categories of data subjects are determined and controlled by the Clients, at their sole discretion.

Categories of personal data transferred

Personal data used by the Clients within the Services including but not limited to any personal data stored by the Clients on, and/or computed by the Clients using, OVH SAS' and OVH European Affiliates' infrastructures. The categories of such personal data are determined and controlled by the Clients, at their sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The categories of such personal data are determined and controlled by the Client, at its sole discretion.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer is determined by the Clients, at their sole discretion.

Nature of the processing

The nature of processing activities carried out by the data importer on personal data may be computing, storage and/or any such other Services as provided in the agreement in force between OVH SAS or the OVH European Affiliates and the respective Client.

Purposes of the data transfer and further processing

Process the personal data to the extent necessary to provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The processing activities are performed for the duration provided in the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

When processors external to the OVH Group are involved in the processing of personal data carried out, this is mentioned in the terms and conditions applicable to the services concerned.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority in accordance with Clause 13

France - Commission Nationale de l'Informatique et des Libertés - CNIL

8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02

Tel. +33 1 53 73 22 22

Spain - Agencia de Protección de Datos

C/Jorge Juan, 6 28001 Madrid

Tel. +34 91399 6200 • e-mail: internacional@agpd.es

Portugal - Comissão Nacional de Protecção de Dados - CNPD

R. de São. Bento, 148-3° 1200-821 Lisboa

Tel. +351 21 392 84 00 • e-mail: geral@cnpd.pt

Italy - Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121 00186 Roma

Tel. +39 06 69677 1 • e-mail: garante@garanteprivacy.it

Germany - Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30 - 53117 Bonn

Tel. +49 228 997799 0 • e-mail: poststelle@bfdi.bund.de

Netherlands - Autoriteit Persoonsgegevens

Prins Clauslaan 60 P.O. Box 93374 2509 AJ Den Haag/The Hague

Tel. +31 70 888 8500 • e-mail: info@autoriteitpersoonsgegevens.nl

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The applicable security principles and rules are defined by the security team in partnership with OVHcloud top management. The security team, under the responsibility of the CISO, is itself composed of 4 teams:

The **security.tools** team in charge of developing the security tool used within OVHcloud. This team designs and operates the tools to support certain security measures deployed on all OVHcloud information systems. These tools include the management of the identities and accesses of employees and service providers, authentication mechanisms made available to clients, identification of vulnerabilities on systems and security monitoring. This team also assists other business teams in the design and deployment of architectures by ensuring security from the definition phase onwards.

The **security.operations** team is responsible for supporting teams in the implementation of good security practices within operations, the implementation of formal security management processes, the support in the integration of security tools and the alignment of security devices within OVHcloud. The security.ops team puts in place an internal control system, both organizational and technical on security and assists the product teams in the implementation of formal information security management systems and in their certification.

The **security.cert** team is responsible for monitoring threat sources, identifying attack tools and methods to anticipate them, and managing malicious security incidents. This team manages the OVHcloud CSIRT and exchanges with international expert communities to provide the best sources of information to anticipate attacks.

The **security.customer** team is in charge of adapting the products offered by OVHcloud to the specific needs of specific business sectors (healthcare, finance, etc.). The team values the expectations of these business sectors, and coordinates OVHcloud's response to contractual and standard compliance. It also provides level 3 support for customer questions about compliance and information security.

The security team is accompanied by the **physical security management teams** and the **privacy teams**. These three teams work together to ensure optimal effectiveness of actions on these subjects with strong adherence.

In addition, security referees are deployed within OVHcloud teams. These focal points enable the dissemination of good practices within teams, provide an identified point of contact for incident and crisis management, and enable the gathering of information from operations to the security team.

A security committee led by the CISO and the managers of the security team ensures communication with the Executive Committee (ComEx) of OVHcloud. This semi-annual committee presents the main threats under surveillance, the major risks, the monitoring metrics, the progress of the ongoing actions and the updated roadmap. This committee also ensures that the ISSP is aligned with OVHcloud's strategic and operational objectives.

Security compliance management

The ISMS aims to ensure that the security requirements of the various interested parties of OVHcloud are taken into account. These requirements are of different kinds:

- legal or regulatory requirements
- contractual commitments
- good practices on which OVHcloud is committed explicitly

OVHcloud must identified and consolidate those requirements and implement the management system in support for the compliance to these requirements.

Documentation

OVHcloud must deploy a formal documented management system to :

- provide a comprehensive framework for policy rules, guideline, operational documentation, records and indicators
- ensure formalism and follow-up of activities implemented to reduce risks
- demonstrate compliance with applicable legal, regulatory or contractual requirements
- demonstrate compliance with the rules set out in the detailed security policies

Assets management

OVHcloud must deploy a formal approach for managing assets carrying security risks or in support for security management to ensure appropriate security controls over them:

- Maintain accurate inventories of those assets
- Define and maintain ownership for those assets
- Classification of those assets based on appropriate criteria to support security decision
- Definition of security rules adapted to their criticality

Security risks management

OVHcloud must deploy a risk management approach to structure operational decisions affecting security. This risk management approach is based on the principles of ISO/IEC 31000 and ISO/IEC 27005 standards. It is based on:

- In-depth knowledge of systems through asset cartography, asset classifications and valuations from a security perspective
- Ongoing analysis of feared events, vulnerabilities, and the threat environment
- uniform formalization of security risks to make them explicit to technical experts and decision-makers for reasonable and informed decision-making
- follow-up of decisions and action plans following the identification of a risk

The establishment of formal risk management enables the operational specificity of a project or product to be taken into account and the achievement of specific security objectives. Failure to comply with a ISSP rule results in an analysis of the risks resulting from the introduction of compensatory security measures to achieve at least an equivalent level of safety or acceptance of risk.

Privacy

The legislation applicable to the protection of personal data and our privacy policy constitute the framework for the processing of this data that OVHcloud applies. ISMS complements this framework by consistently defining, implementing, and improving security arrangements that ensure the protection of hosted personal data.

This commitment is reflected in particular in:

- The implementation of a Personal Information Management System (PIMS) integrated with ISMS
- Setting up a joint management instance between the security and privacy teams
- Alignment of security and data usage policies
- Integrating security measures within ISMS into contractual commitments on personal information protection with customers
- The privacy team's participation in ISMS management
- Involvement of the security team in efforts to identify privacy risks
- Joint participation in resolving security incidents that impact personal information
- Joint definition of security objectives and measures to be implemented in the context of projects.

Customer Protection

OVH implements means of protection on the tools made available to these customers as well as on the communication channels between them and OVHcloud such as: :

- Customer interfaces through the use of identification factors ;
- Tools of detection and alerting when customer credentials are used for illegitimate purpose;
- Protection of customer infrastructures and services against external threats
- data related to customer managed by OVHcloud

Moreover, OVHcloud protects its communications with customers with adequate means according to the context like encrypted channels, collaborative tools with access and security controls or any other means defined with customers.

Customer trust

OVHcloud must provide the adequate transparency to customer in order the assist them in defining the right product for their needs. In particular, OVHcloud must provide information about :

- Physical location of the data and workloads hosting
- Physical location of the control plane and administrators
- Physical location of the support teams
- Applicable law for the service contract
- Supply chain and technical dependencies (Hardware, Software, Subcontractors)
- Reversibility capabilities information
- Certification and assurance mechanisms in place

Customer in cloud security

OVHcloud must produce a clear definition of responsibilities between OVHcloud and customer:

- Assets ownership
- Operations responsibility
- Security risk ownership
- Recommendation of security controls to implement by customer with OVHcloud included features and configuration
- Recommendation of security controls to implement by customer with optional features or external means when relevant

Security Ecosystem

OVHcloud must maintain close relationship with security communities to improve the quality of risk mitigation and accelerate response time to security threats. Security communities are covering but not limited to :

- Security experts, internally and externally
- Security team from hardware manufacturers
- Security team of software editors
- Open source groups
- Security software editors
- Security professional services providers

External technical reputation

OVHcloud must implement a set of processes to ensure the technical reputation of all systems exposed on public networks, since OVHcloud customers are relying on OVHcloud assets for their own information system. This covers:

- IP reputation to ensure that IP allocated to a customer infrastructure are usable for all legitimate purposes
- Abuse process to handle the dispute process when customer infrastructures are used for malicious activities
- Anti-fraud process to ensure all infrastructure usage is legitimate
- Anti-hack process to take down customer compromised infrastructures
- Spam, phishing, malware and dDoS detection and mitigation to protect the public from threats that might be hosted on OVHcloud infrastructure
- Protection and management of all assets under OVHcloud responsibility connected to public networks

Information system user

OVHcloud must protect information and systems by ensuring the information system is adequately operated:

- users are aware of the rules applicable to IS usage
- Company owned device management
- Employee owned device management
- Access to IS from external devices
- Collaborative tools
- Workstation security
- Mobile devices

Human resources

OVHcloud must integrate security topic into HR processes to ensure adapted resources are available to meet security objectives. This includes:

- security investments and human resources related to security priorities
- development of roadmaps of other OVHcloud teams to integrate security needs (investment and human resources)
- skills and training requirements for teams and inclusion in the training plan
- identifying gaps between needs and available resources for the adaptation of roadmaps and taking into account in risk management.

OVHcloud must educate employees on security as soon as they are integrated and throughout their presence in OVHcloud. This awareness is realized by:

- IT policy document to define the rules of usage of information system
- On boarding awareness session for all employees
- Formal threat presentation sessions targeting OVHcloud and security features in place
- Regular communications on good practices and risks
- Communications focused on a specific threat, related to current events or our detection activities
- Tests of the reflexes and the reaction capabilities of the collaborators
- Sharing information resources and feedback on cloud threats and vulnerabilities

OVHcloud must manage security in the complete employee life-cycle:

- Background check fitted to position criticality
- On boarding management including contractual commitment and awareness management
- Specific security training depending of position criticality
- Regular awareness session
- Disciplinary process for security violation
- Termination of contract management

Identity and access management

OVHcloud must maintain a strict policy of logical access rights management for employees :

- all employees use nominative user accounts to access any system
- generic and anonymous accounts is prohibited for any human access
- authorizations are issued and monitored by managers, following the principle of least privilege and the principle of gradually gaining trust
- to the greatest extent possible, all authorizations should be based on roles rather than unit rights
- a formal, fully auditable process is in place for account creation, modification, deletion and password change
- connection sessions systematically have an expiry period suited to each application
- user accounts are automatically deactivated if the password is not renewed after 90 days
- password complexity is mandatory based on best practices and recommendations from authorities:
    - users use automatic password generators rather than choosing their own passwords
    - Complexity rules are defined and communicated to all employees, and when possible technically enforced on systems

    - passwords must be renewed regularly, with a maximum of 90 days
- storing passwords in unencrypted files, on paper or in web browsers is prohibited

OVHcloud must maintain a strict policy of for managing administrator access rights for platforms :

- all administrator access to live systems is realized via a bastion host
- administrators connect to the bastion hosts via SSH, using individual and nominative pairs of public and private keys
- connection to the target system is realized either via a shared service account or via a nominative account and bastion hosts; using default accounts on systems and equipment is prohibited;
- dual-factor authentication is mandatory for remote administrator access and for any employees accessing sensitive areas of the system, with such access being fully traced
- administrators have an account exclusively devoted to administration tasks, in addition to their standard user account;
- authorizations are granted and monitored by managers, in accordance with the principle of least privilege
- SSH keys are protected by a password that meets the requirements of the password policy

Cryptography

- Use strong cryptography to secure data at rest and in transit and administration operations.
    - Manage cryptographic assets with automated process
    - Monitor certificates and keys to ensure all systems have valid certificates at all time

Physical security

OVHcloud physical security is based on zoning. Each area within OVHcloud premises is categorized in a zone type dependent from the area usage and the sensitivity of operations and assets hosted. At each zone type, according to it's sensitivity is defined security controls on:

- Environmental protection against fire, flood, weather conditions our any applicable environmental hazard related to premises location
    - Monitoring of any malicious or accidental events with automated (CCTV, sensors) or human (security watch)
    - Zone control, with a formal definition of all zones interfaces and gateway
    - Access control to ensure only authorized people access each zone for legitimate purpose

Supply Chain

OVHcloud's product teams rely mainly on other OVHcloud teams, but also on partners, subcontractors and suppliers to manage operations, and to compose products and services delivered to customers. The match between the outsourced activities and OVHcloud's security commitment must be managed:

- Identify dependencies between OVHcloud teams and subcontractors, suppliers and partners
    - Classification of criticality dependencies
    - Risk analysis and risk reduction where necessary
    - Service level cascade and security commitments
    - Integrating security into projects
    - Security insurance plan for subcontractors

Architecture

OVHcloud must ensure that cloud architecture is designed to be and stay secure taking into account the complexity of information system required to deliver the service, the factorization of information systems assets to optimize ressources and the management of several generations of technologies. We rely on several pillars to achieve this objective:

- Strong segregation of systems by criticality
- Mutualization of security primitives under the management of security team
- Harmonization of management of specific security assets and processes under common management rules
- Strong automation for security deployment

OVHcloud security team maintain a list of basic security architecture guidelines for systems. Architecture principles must be defined and documented for each type of infrastructure internally. OVHcloud uses several classification scheme for IT architecture depending of needs.

Exemples of classification:

- Tiers 0, Tiers 1, Tiers 2 for internal IS, depending of the internal usage
- Mutualized control plane
- Product dedicated control plane
- Customer infrastructure (Data plane)

Classification scheme must be used to define the set of security controls to apply according to the threat environment relevant to the classification characteristics.

Configuration and hardening

- Use OS patterns with system exposure minimization and baseline of security tools
- Use hardened kernels
- Follow best practices for configuration
- Deploy system as code with automated deployment tools
- Regularly review configurations for security

Administration

OVHcloud maintain those rules for administration activities:

- all administrator access to live systems is realized via a bastion host
- administrators connect to the bastion hosts via SSH, using individual and nominative pairs of public and private keys
- connection to the target system is realized either via a shared service account or via a nominative account and bastion hosts; using default accounts on systems and equipment is prohibited
- dual-factor authentication is mandatory for remote administrator access and for any employees accessing sensitive areas of the system, with such access being fully traced
- administrators have an account exclusively devoted to administration tasks, in addition to their standard user account
- authorizations are granted and monitored by managers, in accordance with the principle of least privilege and the principle of gaining trust

- SSH keys are protected by a password that meets the requirements of the password policy; access rights are reviewed on a regular basis, in collaboration with the departments concerned

Vulnerability and patch management

OVHcloud must ensure a systematic deployment of available security patches within a time frame defined by system based on its criticality. Vulnerabilities on systems must be identified and evaluated as soon as the associated patch is available. The application of the patch outside the predefined time limit must be justified on the basis of the level of risk associated with the corrected vulnerability or the existence of compensatory controls reducing the risk to an acceptable level.

- System owners are responsible of vulnerabilities management of their systems
- Assets shall be classified in terms of criticality
- Patch deployment is based on asset criticality and prioritization of patch deployment is based on risk level
- Vulnerability mitigation can be achieve without patch deployment, in that case, a complete analysis of the situation must be performed

OVHcloud must complete this process by a threat intelligence process and vulnerabilities monitoring to ensure all vulnerabilities that could put systems at risk are mitigated.

Monitoring and detection

OVHcloud must log all records necessary to understand any security events:

- logs are backed up and not limited to local storage
- logs are consulted and analyzed by a limited number of authorized personnel, in accordance with the authorization and access management policy
- tasks are divided up between the teams responsible for operating the monitoring infrastructure and the teams responsible for operating the service

The list of activities that are logged includes the following:

- logs of storage servers hosting customer data;
- logs of the machines managing the customer's infrastructure;
- logs of the machines monitoring the infrastructures;
- logs of the antivirus software installed on all equipped machines;
- integrity checks of logs and systems, where appropriate;
- tasks and events carried out by the customer on their infrastructure;
- network intrusion detection logs and alerts, if appropriate;
- logs of network equipment;
- logs of the infrastructure of the surveillance cameras;
- logs of administrator machines;
- logs of time servers;
- logs of badge readers;
- logs of bastion hosts.

OVHcloud implement tools and process to ensure:

- Fast detection of security events to minimize the occurrence of incidents and minimize impacts
- Adapted capabilities to investigate in post mortem

Change management

OVHcloud must maintain a formal change management principles including security :

- roles and responsibilities in security are clearly defined
- All changes are documented in tracking tool
- criteria for classification are set out in order to identify the security analysis to follow
- the risks associated with the changes are analyzed (if a risk is identified, the security manager and risk manager work together to validate the change)
- intrusion tests may be carried out (where applicable); the change is planned and scheduled with the customers (where applicable)
- the change is rolled out gradually (1/10/100/1000) and, if there is a risk, a rollback procedure is planned
- a retrospective review of the change is carried out

Each unit within OVHcloud implement its own change management procedure according to this principles.

Project management

OVHcloud integrates security within evolution and transformation projects. Compliance with ISSP and data protection is a general requirement for all OVHcloud activities. The security team assists OVHcloud project teams in the full lifecycle of all projects to ensure that the security means are adequate and properly implemented. This support consists of:

- Determine the security criticality of the data and processes involved in the project
    - Accompany project managers in the definition of technical and functional architecture
    - Support project teams in integration into the OVHcloud IS
    - Ensure compliance with the security base in the context of the project and the specific security measures to be put in place
    - Assist sponsors and project leaders in arbitrating specific measures against financial and operational constraints
    - Evaluate the security level of the project before production phase and after go-live
    - Identify residual risks and monitor them over time

Incident management

OVHcloud deploys a unified approach to security incident management by putting in place the organizational and technical means to:

- Detect and consolidate events that can impact the security of information systems and services
    - Correlate events that indicate a possible breach of information security and trigger incident handling as soon as possible
    - Mobilize experts and decision-makers in charge of resolving the incident
    - Support the incident with the following objectives
        - Reduce operational impacts
        - Preserve evidences to support possible judicialization or internal sanctions
        - Return to nominal situation
    - Inform interested parties in accordance with legal and contractual obligations
    - Identify root causes, update risk analysis, and define potential action plans to reduce the risk of a new occurrence

Network security

OVHcloud is managing a worldwide backbone to connect all infrastructures hosted in the datacenters and local networking to ensure the appropriate functioning and administration of the systems. The network security relies on:

- segmentation and segregation of network zones
- all networks equipment's are administered via a bastion host, applying the principle of least privilege
- access to the administration interfaces and administrator features for equipment is reserved to staff listed on control lists
- Network device inventory and automatized management
- Management of traffic and reaction to specific events
- Configuration of networks devices in terms of networking rules and access control
    - Administration of network based on automation. Configurations are deployed automatically, based on validated templates
    - Devices configuration are managed in a central configuration repository
    - A process is in place for ensuring changes are controlled
- the logs are collected, centralized and monitored on a permanent basis by the network operations team

Continuity

Continuity management relies on all mechanisms to ensure Availability, Rescue and Recovery.

Systems criticality must be defined to determine acceptable Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

System owners must implement controls to ensure the effectiveness ot continuity mechanisms.

Internal controls

First-level internal controls are deployed by the operational teams and the security team. These monitoring activities are mainly carried out in the form of:

- automated systems monitoring mechanisms
- operational checkpoints integrated into processes to ensure team coordination, risk accounting, and possible validations of risky activities. Where possible, these control points are integrated into the tools.
- ad hoc operational controls by security experts

Second-level internal control is carried out by the security teams to ensure the effectiveness of the first-level controls. These activities are formal.
The effectiveness of ISMS is also monitored in the context of steering activities.

Internal audits

OVHcloud relies on internal audit approaches to assess the effectiveness of internal control activities. These audits are performed by teams independent of audited operations and systems. Internal audit approaches include:

- Organizational and technical audit of the rules defined within ISSP
- Technical audit of architecture review, deployment, project
- Source code audit
- Intrusion tests

These steps are carried out by OVHcloud personnel or external contractors.

OVHcloud is implementing a public Bug Bounty program that will enable the permanent testing of our systems exposed on the internet.

These activities help identify vulnerabilities, non-conformities and opportunities for improvement and fuel the process of continuous improvement of security.

External audits

OVHcloud implements an external audit program on certified perimeters. We rely on:

- general security framework: ISO 27001, AICPA TSP (SOC)
- Cloud Provider-specific security framework: ISO 27017, CISPE, CSA CCM
- repositories dedicated to specific issues such as privacy: CISPE, ISO 27018, ISO 27701
- industry or geographical specific security framework: PCI DSS, HDS, PSEE, SecNumCloud, AGID, ENS, C5

For each framework, we determine the most appropriate certification or audit organization to strengthen our clients' confidence in our ability to meet the requirements that meet their expectations.

Audits by customers and authorities

OVHcloud allows its customers, under certain conditions, to perform security audits on systems.

Such audits may be:

- Technical, performed remotely (Intrusion Test, Vulnerability Scan) without OVHcloud teams intervention
- Organizational and technical in asynchronous way through questionnaires and written exchanges with OVHcloud
- On-site organizational and technical, including installation visits, interviews with operational staff, and access to documentation and configurations.

As with internal and external audits, these evaluations provide input to the security continuous improvement.

Continuous improvement

OVHcloud is implementing a continuous improvement of security and management processes. Opportunities for improvement are identified by:

- Internal control activities
- Internal and external audits
- Security Incident Analysis
- Identification of security risks

- Stakeholders involved in security management processes
- OVHcloud Security Interested Parties
- Analysis of root causes of non-conformities, vulnerabilities and incidents

These opportunities for improvement are evaluated before implementation and where appropriate prioritized and arbitrated. Consecutive action plans are formally followed in the project management tools used by teams

The processor adopts the same technical and organizational measures as the controller, listed above.