PERSONAL INFORMATION PROTECTION AGREEMENT

Version dated 06.09.2023

This Personal Information Protection Agreement ("**PIPA**") is part of the contract, hereinafter referred to as the "Contract", between Hebergement OVH Inc. ("**OVHcloud"**) and the Client, defining the terms and conditions applicable to the services performed by OVHcloud (the "**Services"** or the "**Service"**). This PIPA and the other provisions of the Contract supplement one another; however, in the event of conflict, the PIPA prevails.

Expressions that begin with a capital letter that are not defined in this PIPA have their meaning defined in the Contract. "Person concerned", "Person in charge of the protection of personal information", "Personal Information", and "Confidentiality Incident" are defined according to the *Act respecting the protection of personal information in the private sector* (CQLR c. P-39.1), hereinafter referred to as the "Quebec Privacy Act". The term "Hosting" refers to all storage, hosting, computing and retention operations performed by OVHcloud, and/or any other Service as described in the Contract.

The purpose of this PIPA is to define the conditions under which OVHcloud is entitled, in the context of the Services defined in the Contract, to carry out, on behalf of and at the instruction of the Client, the Hosting of any Personal Information by the Client within the Services, excluding any Personal Information in the OVHcloud Personal Information Usage Policy, which is collected and used by OVHcloud on its own behalf. For the purposes of the Hosting operations conducted on Personal Information, the Client is deemed to be the company that collects, holds, retains, uses and discloses Personal Information. If the Client is acting on instructions from another company that collects, holds, retains, uses and discloses Personal Information, certain obligations will apply.

1. Scope

1.1 As a service provider, OVHcloud is authorised, upon instruction from the Client, to Host Personal Information entrusted to it to the extent necessary to provide the Services.

1.2 The type of Personal Information and the categories of Persons Concerned are determined and controlled by the Client, at their sole discretion.

1.3 The Hosting is carried out by OVHcloud for the duration set out in the Contract.

2. Service selection

2.1 The Client is solely responsible for selecting the Services. The Client ensures that the Services selected meet the characteristics and conditions required to comply with their own activities and obligations under the applicable law, as well as the type of Personal Information that is the subject of the Hosting, including but not limited to when the Services are used for the retention or destruction of Personal Information that is subject to specific regulations or standards (for example, healthcare or banking data in certain countries).

2.2 If the Client's operations are likely to result in a high risk to the rights and freedoms of natural persons, the Client must carefully select their Services. In assessing risk, the following non-exhaustive criteria shall be taken into account: projects involving new technologies or biometric, health or sensitive data; projects characterised by a volume of Persons Concerned or hosted Personal Information; or projects containing ethical issues, such as academic, medical, scientific or statistical research.

2.3 OVHcloud shall make available to the Client information relating to the security measures implemented, in the manner set out below in the "Audits" chapter, as part of the Services, to the extent necessary to assess the compliance of these measures with the Client's activities.

3. Compliance with applicable regulations

Each Party shall comply with its applicable laws on the protection of Personal Information (including the Quebec Privacy Act and the *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, c. A-2.1), hereinafter referred to as the "Quebec Access Act").

4. OVHcloud's obligations

4.1 OVHcloud agrees to:

a) Not access or use Personal Information for any purposes other than those necessary to perform the Services (including in connection with managing Privacy Incidents),
b) Implement the measures for the protection of Personal Information described in the Contract, in order to ensure the security and confidentiality of Personal Information within the Service,
c) Ensure that OVHcloud employees authorised to access Personal Information under the Contract are subject to a confidentiality obligation and receive appropriate training regarding the protection of Personal Information,
d) Authorise OVHcloud employee access to Personal Information only if it is necessary for them to perform their duties,
e) Inform the Client if, in its opinion and in the light of the information at their disposal, an instruction from the Client violates the applicable laws.

4.2 In the event of requests received from judicial, administrative or other authorities to obtain the disclosure of Personal Information hosted by OVHcloud under this PIPA, OVHcloud shall make 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 manifestly incompetent and invalid, (iii) limit the disclosure to Personal Information required by the authority and (iv) inform the Client in advance (unless prohibited by applicable law).

4.3 If the request to obtain the disclosure of Personal Information hosted by OVHcloud under this PIPA on behalf of a Canadian Client originates from an authority outside of Canadian jurisdiction, OVHcloud shall object to the request, subject to the following exceptions:

(a) The request is made in accordance with an international agreement, such as a mutual legal assistance treaty, in force between any combination of the following countries: (i) the requesting country and Canada; or ii) the requesting country and the country where the Personal Information is hosted (as selected by the Client at the time of order submission).
b) The requested Personal Information is hosted in a datacentre located outside of Canada (as selected by the Client at the time of order submission);
(c) The request pursues a significant reason of public interest or is necessary to safeguard the vital interests of the Person Concerned or other persons.

4.4 At the written request of the Client, OVHcloud shall provide the Client with reasonable assistance in carrying out privacy impact assessments if the Client is required to do so under the applicable privacy

law, and in each case only to the extent that such assistance is required and relates to the Hosting operations carried out on Personal Information by OVHcloud under the Contract (including this PIPA). This assistance will consist of ensuring transparency on the security measures implemented by OVHcloud for its Services.

4.5 OVHcloud agrees to implement the following measures to protect Personal Information:

(a) Physical security measures designed to prevent unauthorised persons from accessing the Services where the Client's data is hosted,
(b) Identity and access controls using an authentication system and a password policy,
(c) An access management system that limits premises access to persons who need access to them for the performance of their duties and responsibilities,
(d) Security personnel responsible for monitoring the physical security of OVHcloud premises,
(e) A system for physically and logically keeping Client data separate from one another,
(f) User and administrator authentication processes, and measures to protect access to administrative functions,
(g) An access management system for support and maintenance operations that operates on the principle of least privilege and on a "need to know" basis, and
(h) Processes and measures for tracing the actions performed on its information system.

4.6 These measures to protect Personal Information are detailed on the OVHcloud website and may change over time.

5. Confidentiality incident

5.1 If OVHcloud becomes aware of a Confidentiality Incident affecting the Client's Personal Information or of any breach or attempted breach by any person of the obligations relating to the confidentiality of the information communicated, OVHcloud shall inform the Client's Person in charge of the protection of personal information as soon as possible and in a timely manner.

5.2 The notification shall (i) describe the circumstances of the Confidentiality Incident and, if known, its cause; (ii) describe the Personal Information to which the incident relates, if known; (iii) indicate the date or period when the incident occurred or, if not known, an estimation of that period; (iv) indicate the date or period when the incident occurred or, if this is not known, an estimation of that period; (v) indicate the number of people affected by the incident or, if not known, an estimation of this number, (vi) describe the likely consequences of the incident; (vii) describe the measures taken or planned by OVHcloud in response to the incident; and (viii) provide the OVHcloud point of contact.

6. Location and transfer of Personal Information

6.1 Where a Service allows the Client to host Content, and in particular, Personal Information, the location(s) or geographical area(s) of the available Datacentre(s) are specified on the OVHcloud Website. If several locations or geographical regions are available, the Client shall select the location(s) of their choice when submitting their Order. Subject to any provisions to the contrary in the applicable Specific Terms of Service, when submitting the Order OVHcloud shall not modify the location or geographical area chosen without the Client's prior consent.

6.2 Subject to the previous provision regarding the location of the Datacentres, the OVHcloud affili, excluding entities located in the US, may carry out operations aimed at ensuring the availability of the Services hosting the Client's Content as well as their security or maintenance.

6.3 The Client is responsible for (i) assessing the legality of the location of any Personal Information and of activities carried out remotely as set out in Section 6.2 of this PIPA (including measures to

protect relevant Personal Information), taking into account in particular the categories of Personal Information that the Client intends to host as part of the Services. OVHcloud agrees to assist the Client on request by providing any information in its possession as soon as possible that may be useful for the Client's assessment.

7. Client obligations

7.1 If the Client is acting on instructions from another company that holds the Personal Information, the Parties expressly agree to the following terms and conditions:

a) The Client shall ensure that (i) the necessary authorisations to enter into this PIPA, including the Client's designation of OVHcloud as a service provider, have been obtained from the other company that holds the Personal Information; (ii) an agreement has been entered into with that other company which fully complies with the terms and conditions of the Contract, including this PIPA; (iii) all instructions received by OVHcloud from the Client in execution of the Contract and this PIPA fully comply with the instructions of this other company; and (iv) all information communicated or made available by OVHcloud under this PIPA is communicated appropriately to this other company, if necessary;
b) OVHcloud (i) hosts Personal Information only upon instruction from the Client, and (ii) receives no instruction directly from the other company that holds the Personal Information, except in cases where the Client has effectively disappeared or ceased to legally exist without a successor entity taking on the Client's rights and obligations;
c) The Client, who is fully responsible to OVHcloud for the proper fulfilment of the legal obligations of the other company that holds the Personal Information, shall indemnify and absolve OVHcloud from (i) any failure of the other company that holds the Personal Information to comply with the applicable law, and (ii) any action, claim or complaint from the other company that holds the Personal Information regarding the provisions of the Contract (including this PIPA) or any instructions received by OVHcloud from the Client.

7.2 The Client is responsible for ensuring that:

a) The hosting operations carried out on the Personal Information as part of the performance of the Service are in accordance with the applicable laws;
b) Logical measures are in place to protect the Personal Information Hosted by OVHcloud, such as encryption, even during the transit of Personal Information;
c) Any required procedures and formalities (such as privacy impact assessments) have been completed;
d) The Persons Concerned are informed of the hosting of their Personal Information by OVHcloud in a concise, transparent, intelligible and easily accessible form, in clear and simple language as provided for by the Quebec Privacy Act and the Quebec Access Act;
e) Personal Information is collected, used, disclosed and retained by the Client in accordance with applicable law;
f) The Persons Concerned shall be informed and shall at all times have the possibility to easily exercise their rights, in accordance with the applicable law;

7.3 The Client is responsible for implementing the appropriate Personal Information protection and privacy measures to ensure the security of resources, systems, applications and operations that are not within OVHcloud's scope of responsibility as defined in the Contract (including any system and software deployed and operated by the Client or Users within the Services).

8. Rights of Persons Concerned

8.1 The Client's Person in charge of the protection of personal information is fully responsible for informing the Persons Concerned of their rights, and for respecting those rights, including the rights to access, rectify, erase, limit, or portability of their Personal Information.

8.2 OVHcloud shall provide all the reasonable cooperation and assistance necessary to respond to the requests of the Persons Concerned. This reasonable cooperation and assistance may consist of (a) communicating to the Client any request received directly from the Person Concerned and (b) allowing the Client to design and deploy the necessary measures to protect Personal Information to respond to the requests of the Person Concerned. The Client's Person in charge of the protection of personal information must respond to these requests.

8.3 The Client acknowledges and accepts that, in the event that such cooperation and assistance requires significant resources from OVHcloud, this effort will be billed upon prior notification to and in agreement with the Client.

9. Deletion and return of Personal Information

9.1 Upon expiration of a Service (particularly in the event of termination or non-renewal), OVHcloud agrees to permanently delete, in the manner set out in the Contract, all Content (including information, data, files, systems, applications, websites and other elements) that is reproduced, stored, hosted or otherwise used by the Client in the context of the Services, unless requested by a competent legal or judicial authority, or otherwise provided for by law. However, OVHcloud makes no commitment to store the Content after a Service expires. In any event, the personal information hosted by the Client is deleted within 30 days after the Service is terminated.

9.2 The Client is solely responsible for ensuring that the necessary operations (such as backup, transfer to a third-party solution, retention of Personal Information) are carried out, in particular before the termination or expiry of the Services, and before carrying out any deletion, update or reinstallation of the Services.

9.3 In this regard, the Client is informed that the termination and expiry of a Service for any reason (including but not limited to non-renewal), as well as certain operations that may be performed by the Client to update or reinstall the Services, may automatically result in the irreversible deletion of any Content (including information, data, files, systems, applications, websites and other elements) that is reproduced, stored, hosted or otherwise used by the Client as part of the Services, including any potential backups.

10. Liability

10.1 OVHcloud can only be held liable for damages caused by operations in which (i) it has not complied with the obligations of Quebec Privacy Act and Quebec Access Act specifically related to the performance of the Services or (ii) it has acted in contravention to the legal written instructions of the Client. In this case, the liability provision of the Contract applies.

10.2 Where OVHcloud and the Client are involved in operations relating to Personal Information under the Contract that have caused damage to a third party (including but not limited to the Person Concerned), the Client shall, first, assume the full indemnification (or any other indemnification) that is due to the third party and, second, shall claim from OVHcloud the part of the third-party

indemnification corresponding to OVHcloud's share of the responsibility for the damage provided, provided that any limitation of liability under the Contract applies.

11. Audits

11.1 OVHcloud shall make documentation relating to the Services available to the Client on the OVHcloud Sites, including information on how to host Personal Information.

11.2 If a Service is certified or subject to specific audit procedures, OVHcloud shall make the corresponding certificates and audit reports available to the Client upon written request. Audit reports or other confidential documentation may be subject to a confidentiality agreement before they are made available.

11.3 If necessary and required under the applicable privacy laws, OVHcloud shall authorise the Client's Person in charge of the protection of personal information or any competent person authorised by the Client to conduct an audit regarding OVHcloud's compliance with the privacy obligations set out in this PIPA. In such a case, the Client must give OVHcloud at least 30 days' written notice. OVHcloud reserves the right to remove any auditor on legitimate grounds. In this case, the Client may appoint another auditor.

11.4 OVHcloud and the Client shall agree in writing on the scope and manner in which this audit will be carried out, which shall under no circumstances result in the disruption of OVHcloud's activities. It is preferable that the duration of the audit does not exceed two working days (during OVHcloud's normal business hours). All costs relating to this audit, including OVHcloud's, must be fully borne by the Client and will be billed by OVHcloud to the Client in accordance with the prices in effect at the time the audit is conducted.

11.5 The Client and the entities or persons authorised by them shall make a written commitment not to disclose the information collected as part of the audit, regardless of the method of acquisition under the manners acceptable to OVHcloud, and the signing of this agreement shall be made prior to the audit. The audit report must be made available to OVHcloud before it is finalised, so that OVHcloud can submit all of its observations, with the final report taking into account and responding to these observations.

11.6 The Client's Person in charge of the protection of personal information may not audit more than once in any twelve (12) month period, with the exception of any additional audit or verification (i) that the Client considers reasonably necessary due to a Confidentiality Incident suffered by OVHcloud, or (ii) that the Client is required to perform in accordance with applicable Personal Information Protection laws.

12. Contact OVHcloud

For any questions relating to Personal Information (Confidentiality Incident, Terms of Use, Retention, Disposal etc.), the Client may contact OVHcloud as follows:

(a) By creating a ticket in the Client Account Management Interface,

(b) By contacting their OVHcloud Support team,

(c) By mail to: Privacy Officer, OVH Hebergement Inc., 1801 McGill College Avenue, Suite 800, Montréal, Quebec H3A 2N4