DATA PROCESSING AGREEMENT

ARTICLE 1 - PURPOSE OF THE AGREEMENT

1.1. This Data Processing Agreement ("**Agreement**") supplements the provisions of Article 12 of the General Terms of License and Service (https://www.seald.io/fr/licence-service-agreement-sdk) and is an integral part of the Contract, as that term is defined within the General Terms and Conditions of License and Service.

The purpose of this Agreement is to define the obligations of the Parties with respect to the processing of personal data carried out by Seald in the performance of the Agreement, as a data processor acting on behalf of and on the instructions of the Client, who is responsible for the processing, and determining its purposes.

1.2. In this Agreement, "**Processor**" means Seald and "**Controller**" means Client.

Other words and expressions used shall have the meaning ascribed to them, where applicable, by the applicable regulations on the protection of personal data, including: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**GDPR")**, and, where applicable, (ii) any other national or EU legislation or regulation applicable during the term of the Contract, including French Law No. 78-17 of 6 January 1978 as amended (hereinafter together the "**Personal Data Regulations"**).

ARTICLE 2 - INSTRUCTIONS FROM THE DATA CONTROLLER

2.1. The characteristics of the processing of personal data that the Processor implements on behalf of the Controller, as well as the instructions of the latter at the date of the conclusion of the Agreement, are detailed in the Annex to this Agreement (hereinafter the "**Processing Instructions"**).

During the term of the Contract, the Controller undertakes to formulate and, if necessary, to update in writing the Processing Instructions and more generally to document in writing any additional instructions relating to the processing expected of the Processor in performance of this Contract, which shall also constitute Processing Instructions. Processor shall not be liable for failure to comply with any instruction that has not been documented in writing by the Controller.

The Processor will process personal data solely in the context of the execution of the Contract, the Processing Instructions and any other documented instructions of the Controller, unless it is required to do so otherwise under the Personal Data Regulations. In such a case, he will inform the Controller of this obligation prior to its implementation unless the relevant regulation prohibits such information.

2.2. Prior to the transmission of the Processing Instructions, the Controller declares and guarantees that it has ascertained the lawfulness of the characteristics of the processing operations covered by this Agreement with regard to the Personal Data Regulations, particularly with regard to the purposes of the processing, the determination of the legal basis, the information and, if applicable, the obtaining of the consent of the data subjects, as well as the definition of the duration of storage.

2.3. Without prejudice to the provisions of Article 2.2, if the Processor considers that a Processing Instruction constitutes a violation of the Personal Data Regulations, it will inform the Controller. However, the Processor shall not be obliged to carry out in-depth legal analyses of the Processing Instructions. The parties may exchange positions, but the final decision will be made by the Controller under its sole responsibility.

ARTICLE 3 - CONFIDENTIALITY AND SECURITY OF PERSONAL DATA

3.1. The Processor shall ensure that the persons under its responsibility and authorized to process such information undertake to respect its confidentiality or are subject to a legal obligation of confidentiality.

3.2. The main technical and organizational security measures implemented by the Processor as of the date of signature of the Contract are described in the Security Policy (https://docs.seald.io/reference/architecture/internal-security.html).

The Processor may make changes to these measures during the term of the Contract provided that it maintains an equivalent or higher level of security adapted to the nature of the risks. The Processor undertakes to communicate updates to the security measures upon written request by the Controller.

3.3. The Processor undertakes to notify the Controller of any breach of personal data relating to the processing operations covered by the Agreement, as soon as it is informed. This notification shall be accompanied, as far as possible, by all useful information available to the Processor in order to enable the Controller to assess the nature and consequences of the data breach, to notify the competent supervisory authority and, where applicable, the data subjects. It is the sole responsibility of the Controller to notify, where appropriate, the competent data protection authority and the data subjects of any personal data breach.

ARTICLE 4 - INFORMATION AND RIGHTS OF THE DATA SUBJECTS

4.1 It is the sole responsibility of the Controller to inform the persons affected by the processing operations of the manner in which their personal data will be processed and of their rights, in accordance with the Personal Data Regulations.

4.2. Without prejudice to the provisions of the preceding paragraph, the Processor shall use its best efforts to collaborate with the Controller to help it meet the requirements of the Personal Data Regulations, in particular with regard to the technical content of the information provided to the data subjects and the exercise of their rights by the latter. In the latter case, the Processor undertakes to transmit without delay to the Controller any request received from the data subjects concerning the exercise of their rights, as well as the information enabling the Subcontractor to respond to such requests, insofar as it is available. Any intervention requested from the Processor by the Controller in relation to the management of the exercise of the rights of the data subjects will be carried out at the expense of the Controller if it involves processing time in excess of two (2) hours.

ARTICLE 5 - SUBSEQUENT PROCESSORS

5.1. The Controller generally authorizes the Processor to use subcontractors, subject to the following.

The list of sub-processors is presented for each processing operation in the Processing Instructions. The Processor shall inform the Controller in writing before any modification of this list, subsequent to the conclusion of the Contract. The Processor shall have a period of five (5) working days following the transmission of this information in order to raise any written and reasoned objections regarding the proposed modification. In the event that the Controller objects to the addition of a subsequent sub-processor that is essential for the purposes of the provision by the Processor of the services requested by the Controller, on the grounds of expertise, material capacity, market positioning and/or any other objective criteria communicated by the Processor to the Controller, the Processor shall not be held liable in the event of impossibility or failure in the provision of all or part of the services concerned.

5.2 Any contract between Processor and a subsequent sub-processor shall require the subsequent sub-processor to have obligations at least equivalent to those set forth in this Agreement.

ARTICLE 6 - TRANSFERS OUTSIDE THE EUROPEAN UNION

The following conditions must be met prior to any transfer by the Processor of personal data processed on behalf of the Controller to a country outside the European Union which has not been the subject of an adequacy decision by the European Commission:

- Obtain written authorization from the Controller. On the day of signing the Agreement, the Controller gives his authorization for the transfers described in the Processing Instructions;

- Implement one of the appropriate safeguards referred to in Article 46 of the GDPR;

- If necessary, put in place additional technical and/or organizational measures to ensure that the rights of individuals whose personal data are transferred to a third country are effectively protected at a level substantially equivalent to that guaranteed within the European Union, taking into account the risks identified with regard to possible access by the public authorities of the third country concerned following analysis of the relevant elements of that country's legal system.

ARTICLE 7 - FATE OF PERSONAL DATA UPON TERMINATION OF THE CONTRACT

Upon expiration of the processing periods specified in the Processing Instructions, and in any event upon termination of the Agreement, Processor shall delete all personal data processed under this Agreement, or return such data to the Controller or its designee, as the latter may elect in writing.

At the end of these operations, the Processor will destroy the existing copies, without prejudice to the right of the Processor to temporarily archive all or part of the personal data processed within the framework of this Agreement, to enable it to provide proof of the proper performance of its contractual obligations, or to comply with a legal obligation of conservation.

ARTICLE 8 - COOPERATION AND PROOF OF COMPLIANCE OF PROCESSING

8.1 The Processor shall use its best efforts to assist the Controller in carrying out impact analyses relating to data protection and, where applicable, in prior consultation with the competent protection authority. The costs associated with the intervention of the Processor in this context shall be borne by the Controller and shall give rise to the drawing up of a prior estimate by the Processor.

8.2. The Processor shall provide the Controller, within a reasonable period of time and upon written request from the Controller, all information in its possession that is necessary to establish the compliance of the personal data processing operations it carries out under this Agreement.

8.3. Subject to the conditions set forth below, the Processor agrees to cooperate with the Controller, upon the latter's written request, in the performance of audits and inspections to verify the Processor’s compliance with its obligations under this Agreement.

The Controller may perform a maximum of one (1) audit or inspection per contract year. However, this limit does not apply in the event of a security incident resulting in a data breach. In such a situation, the Controller may carry out a specific audit or inspection following the security incident, without prejudice to the possibility of carrying out a second audit or inspection during the same contractual year.

The Controller must inform the Processor, by registered letter with acknowledgement of receipt, of the audit and of the planned verification operations, giving at least thirty (30) working days' notice before the audit begins. This notice period may be reduced to fifteen (15) business days in the event of an audit following a security incident that has resulted in a data breach. If an external auditor is used, the auditor must not engage in any activity that competes with that of the Processor. Prior to the audit, the Controller and the auditor will sign a confidentiality agreement. The auditor will undertake in particular to use the information communicated in the context of the audit only for the strict requirements of the audit.

The Controller shall bear the costs of the audits or inspections that it decides to carry out. The operations carried out by the processor for the purposes of carrying out the audit or inspection will be subject to a prior estimate which must be accepted by the Controller before the Processor undertakes the said operations.

8.4 The audit report shall be sent to the Processor within fifteen (15) business days of the completion of the audit. Processor shall have the opportunity to comment on the audit report within fifteen (15) business days, which shall be included in the final audit report. The Parties will meet and discuss any measures to be implemented following the audit.

Appendix
Treatment Instructions

*

Note:

- Processing No. 1 corresponds to the processing of personal data necessary for the operation of the Solution in its basic configuration;

- Processing operations no. 2 and 3 correspond to the processing operations necessary for the functioning of the optional plug-ins of the Solution. This processing is only carried out by the Processor in the situation where the Controller uses the corresponding plug-ins.

<table>
<tr><th colspan="3">Treatment 1 - Operation of the Seald-SDK Solution</th></tr>
<tr><td>Object</td><td colspan="2">Processing required for the operation of the Seald-SDK Solution</td></tr>
<tr><td>Nature</td><td colspan="2">Collection, recording, storage, organization, encryption and decryption, access, use, disclosure by transmission and deletion operations.</td></tr>
<tr><td>Purposes</td><td colspan="2">Operation of the Seald-SDK Solution as described in the Agreement and Documentation, including end-to-end data encryption and fraud prevention.</td></tr>
<tr><td>Categories of personal data</td><td colspan="2">- Identification data (identifier used within the Application, public keys, IP addresses) ;
- Administration Panel Login Data;
- Location data (approximate geolocation inferred from the IP addresses of the Users of the Seald-SDK Solution);
- Personal Data that may be included by the Controller in the metadata relating to Encrypted Data or the creation of an Identity for a User.</td></tr>
<tr><td>Data subject</td><td colspan="2">- Users of the Seald-SDK Solution;
- Persons concerned by the personal data that may be included by the Controller in the metadata relating to the Encrypted Data or the creation of an Identity for a User.</td></tr>
<tr><td>Term</td><td colspan="2">Duration of the Contract</td></tr>
<tr><td rowspan="8">Subsequent sub-processors</td><td colspan="2">Subsequent sub-processor n° 1</td></tr>
<tr><td>Name</td><td>OVHCloud SAS</td></tr>
<tr><td>Mission</td><td>Hosting</td></tr>
<tr><td colspan="2">Subsequent sub-processor n° 2</td></tr>
<tr><td>Name</td><td>Scaleway SAS</td></tr>
<tr><td>Mission</td><td>Logging server</td></tr>
<tr><td colspan="2">Subsequent sub-processor no. 3</td></tr>
<tr><td>Name</td><td>Scaleway SAS</td></tr>
<tr><td>Mission</td><td>Backup</td></tr>
</table>

Transfers outside the EU to countries without an adequacy decision	None

Treatment 2 - Plug-in 2-man-rule		
Object	Processing required to operate the 2-man-rule plug-in (two-factor authentication).	
Nature	Collection, recording, storage, organization, access, use and deletion operations.	
Purposes	Enable two-factor authentication of Users of the Seald-SDK Solution.	
Categories of personal data	- Contact data (email addresses, phone number); - Personal data that may be included by the Client in the metadata relating to the use of the 2-man-rule plug-in.	
Data subjects	- Users of the Seald-SDK Solution; - Persons concerned by the personal data that may be included by the Data Controller in the metadata relating to the use of the 2-man-rule plug-in.	
Term	Duration of the Contract	
Subsequent sub-processors	Subsequent sub-processor	
	Name	AC PM LLC
	Mission	Automatically send emails to Users of the Solution allowing two-factor authentication.
	Subsequent sub-processor	
	Name	OVHCloud SAS
	Mission	Automatic sending of SMS to Users of the Solution allowing two-factor authentication.
Transfers outside the EU to countries without an adequacy decision	United States (AC PM LLC) - Transfer governed by transfer clauses based on the standard contractual clauses published by the European Commission.	

Process 3 - Seald Secure Key Storage	
Object	Processing required for the operation of the SSKS plug-in
Nature	Collection, recording, storage, organization, access, use and deletion operations.
Purpose	Backup of Users' private identity keys
Categories of personal data	Identification data (private keys).
Data subjects	Users of the Solution
Term	Duration of the Contract
Subsequent sub-processors	Subsequent sub-processor n° 1

	Name	OVHCloud SAS
	Mission	Hosting of Users' private identity keys (noting that these keys are encrypted and not stored in clear text)
	Subsequent sub-processor n° 2	
	Name	Scaleway SAS
	Mission	Logging server
	Subsequent sub-processor no. 3	
	Name	Scaleway SAS
	Mission	Backup
Transfers outside the EU to countries without an adequacy decision	None	