

Annex 1: Data Processing Agreement

Introduction

- A. This Data Processing Agreement (“**DPA**”) is incorporated into, and is subject to the terms and conditions of, the Software License Agreement (“**Agreement**”) between Klippa App B.V. (“**Klippa**” or “**we**”) and the Licensee entity that is a party to Agreement (“**Licensee**” or “**you**”). Klippa and the Licensee will hereinafter (also) be individually referred to as a “**Party**” and collectively as the “**Parties**”.
- B. Klippa, when Processing Personal Data in the context of the performance of the Agreement, can be considered a ‘Processor’ within the meaning of the General Data Protection Regulation (EU) 2016/679 (the “**GDPR**”) and the Licensee can be considered a ‘Controller’ within the meaning of the GDPR.
- C. The Parties, given the obligations stated in the GDPR and additional member state law to which the Licensee is subject in addition thereto (hereinafter collectively referred to as the: “**Applicable Privacy Law**”), wish to record their rights and obligations in writing by means of this DPA.
- D. In this DPA, the terms ‘Personal Data’, ‘Processing’, ‘Data Subject’, ‘Sub-processor’, ‘Purpose’ and ‘Personal Data Breach’ shall have the same meaning as set out in the GDPR and should be interpreted in accordance with the GDPR.

1. Personal Data to be processed

Klippa undertakes to Process the Personal Data, Processed in the context of the performance of the Agreement, on the terms and conditions of this DPA. The nature and the Purpose of the Processing, as well as the type of Personal Data and categories of Data Subjects processed by Klippa on behalf of Licensee, is set out in the Agreement, in the absence of which the processing is limited to those activities strictly necessary for the performance of the Agreement.

Notwithstanding the aforementioned, Klippa is allowed to process the Personal Data to the extent that Klippa is required to do so by either Union or member state law to which Klippa is subject. In such a case, Klippa shall inform Licensee of that legal requirement before processing, unless that law prohibits providing such information on important grounds of public interest

2. Role of Parties

Klippa shall only process the Personal Data on documented instructions from Licensee. Licensee is deemed to have given the instructions to Klippa for any processing strictly necessary for the provisioning of the services described in the Agreement. These instructions include the processing that results out of changes to these services, to the extent the Agreement allows for such changes.

3. Confidentiality

Klippa shall keep confidential all the Personal Data and other confidential information, and shall not make it public, other than to the extent necessary for the provision of the services or insofar as Klippa is legally obliged or ordered by a court to disclose and/or

supply the Personal Data. Klippa will agree to the same conditions for confidentiality with the persons who have access to the Personal Data (e.g., Klippa personnel).

4. Security measures

Preserving the confidentiality and integrity of Licensee's information is one of Klippa's highest priorities. Klippa has technical and organizational measures in place to ensure a level of security appropriate to the risk, including the Klippa Security Policy. These measures shall be appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context and Purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The most recent version of the overview of all the security measures that Klippa undertakes can be requested via email.

The nature of the provision of services – the delivery and implementation of standard software – entails that there are limited possibilities for taking specific measures for a Licensee, in addition to the standard security measures as mentioned above. Klippa is therefore only obliged to take such measures tailored to the Licensee if this has been expressly agreed between the Licensee and Klippa. Klippa is allowed to change the mentioned measures as it deems fit.

Klippa shall periodically test, assess and evaluate the effectiveness of the technical and organisational measures taken to secure the Processing, whether or not by calling in an expert third party. Such assessments might result in changes in the measures taken.

Klippa shall take all necessary steps to ensure that any natural person acting under Klippa's authority, who has access to Personal Data, does not process this Personal Data except on instructions from Licensee, unless he or she is required to do so by Union or Member State law.

5. Personal Data Breaches

In the case that Klippa encounters a Personal Data Breach which impacts your data security, Klippa will inform you without any unreasonable delay, but in any case, within 72 hours, as soon as Klippa has taken note of it. This notification shall at least, to the extent Klippa has the information:

- A. describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- B. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- C. describe the likely consequences of the Personal Data Breach;
- D. describe the measures taken or proposed to be taken by the controller to address the Personal Data Breach, including, where appropriate, measures to mitigate Klippa possible adverse effects;
- E. provide Licensee with any other information Licensee needs according to the Applicable Privacy Law.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Klippa shall assist Licensee in ensuring compliance with the obligations pursuant to the Applicable Privacy Law, taking into account the nature of Processing and the information available to the processor. This also includes assisting Licensee in informing the Data Subjects about Personal Data Breaches.

Klippa shall document any Personal Data Breaches, including the facts relating to the Personal Data Breach, the consequences thereof and the corrective actions taken, as well as any other relevant information regarding the Personal Data Breach.

Klippa will make every effort to take effective measures in the event of a Personal Data Breach in order to undo the negative consequences resulting from the Personal Data Breach as much as possible and to limit any further negative consequences as much as possible.

6. Hosting & storage

Klippa shall process (or arrange the Processing of) the Personal Data solely within the European Economic Area (“**EEA**”), unless (i) Licensee authorizes or instructs the transfer of Personal Data outside the EEA or (ii) Klippa is required to transfer the data by the Applicable Privacy Law to which Klippa is subject.

Klippa does not store any personal information. We do store logs of API Calls that encountered an error. We delete them when they are reviewed by one of our colleagues and no later than thirty days, whichever event happens first.

7. Sub-processors

Licensee agrees that Klippa may engage Sub-processors to process Personal Data on Licensee’s behalf. The Sub-processors currently engaged by Klippa and authorized by Licensee are available via the following URL:

<https://link.klippa.com/subprocessors>

Klippa shall notify Licensee if it adds or removes Sub-processors at least thirty (30) days prior to any such changes. Licensee may object in writing to the Processing of its Personal Data by a new Sub-processor within thirty (30) following the notification of this policy and such objection shall describe Licensee’s legitimate reason(s) for objection. If Licensee does not object during such time period the new Sub-processor(s) shall be deemed accepted.

If Licensee objects to the use of the new Sub-processor pursuant to the aforementioned process, Klippa will have thirty days to decide to cease using this new Sub-processor or appoint a new Sub-processor with regard to the Processing of Personal Data on behalf of Licensee. In case that solution is not satisfactory, Licensee may suspend or terminate the DPA, and subsequently the Agreement. Further termination rights, as applicable and agreed, are set out in the Agreement.

When engaging a Sub-processor:

- A. Klippa remains fully liable for the fulfilment of the obligations under this DPA;
- B. Klippa will lay down the engagement of the Sub-processor in an appropriate sub-processing agreement;
- C. The aforementioned agreement will contain clauses to address Licensee's compliance pursuant to the Applicable Privacy Law in a materially similar way.

8. Data Subjects rights

Licensee is Processing Personal Data from its Licensees, partners and suppliers (Data Subjects) using Klippa, possibly amongst other systems. The Applicable Privacy Law grants certain rights to the Data Subjects. The responsibility for dealing with (the exercise of) these rights rests at Licensee.

However, Klippa will, if requested by Licensee, provide Licensee with all reasonable cooperation in the fulfilment of Licensee's obligations on the basis of the rights of Data Subjects at the Licensee's expense. Klippa cannot guarantee that it can always provide the cooperation within the time frames specified in the Applicable Privacy Law that bear on Licensee.

9. Information, cooperation, audit and compliance

Klippa shall make available to Licensee all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Licensee in order to assess compliance with this DPA.

If Licensee wants to have an audit performed, you have to let Klippa know at least 30 days beforehand. Any audit will always be performed at a day and time that is favorable to Klippa. Audits can only take place by an independent auditor that is a member of NOREA. Both you and your auditor are bound by a full non-disclosure agreement on the process and outcome of the audit. Any cost, directly or indirectly, accompanied with an audit is to be paid by Licensee. Licensee is not allowed to carry out such an inspection more than once per contract year.

At Licensee's expense, Klippa will assist Licensee in ensuring compliance with its obligations pursuant to the Applicable Law.

10. Limitation of liability

Any limitation of liability specified in the Agreement(s) applies *mutatis mutandis* to this DPA. If as a result of an attributable shortcoming by Klippa, or an act or omission attributable to Klippa, a penalty is imposed on Licensee by a government supervisor, which penalty is directly related to the aforementioned shortcoming, act or omission,

Klippa indemnifies Licensee for (that part of) that fine. For clarity: the indemnity does not apply to the part of the fine that is related to the behaviour of Licensee himself. The limitation of liability as specified in the Agreement applies to this indemnification. Any limitation of liability will lapse in case of intent or gross negligence on the part of Klippa.

11. Consequences of Applicable Privacy Law

As a Controller, Licensee is responsible and accountable for the Personal Data you are Processing using the services of Klippa. Therefore, the responsibility for compliance with the Applicable Privacy Law, in the Processing of Personal Data in relation to the Agreement(s) rests at Licensee. Licensee warrants that the Processing of Personal Data pursuant to the Agreement complies with the Applicable Privacy Law and will indemnify and hold harmless Klippa for any claims from any third party that are based on a breach of the aforementioned warranty.

12. Term, termination and consequences of termination

This DPA shall be in force for the same duration as the Agreement. This DPA shall automatically terminate once all Agreements are terminated. Klippa will not store the Personal Data that it processes in relation to the services for a longer period than necessary for the performance of its obligations under the Agreement. General principle is that the storage of data is no longer necessary after the provision of the services under the Agreement has been completed. This means that Personal Data will in principle be destroyed by Klippa after the agreed services have been completed. Klippa is explicitly not obliged to save the Personal Data for a longer time. Licensee is responsible for meeting any storage and administration obligations.

13. Applicable law and competent court

Dutch law applies to this DPA. Except insofar the Agreement designates an exclusively competent court, the court located in the district where Klippa is domiciled (Groningen, The Netherlands) has exclusive jurisdiction.