TEMPLATE DATA PROCESSING AGREEMENT (DPA)

This is a template of a data processing agreement ("DPA"). If you are looking for other template models, check out our website (www.penrose.law/downloads).

This template takes the position of the *controller* as the starting point. If you are looking for a processing agreement that takes the position of the *processor* as the starting point, or an agreement for *joint controllers*, please contact us.

This model contains the standard and most common provisions in a processing agreement, in accordance with the European General Data Protection Regulation ("GDPR"). Within the framework of the GDPR, variations and additions to the text and the provisions remain possible. For a more tailor-made agreement, do not hesitate to contact us. The parts that still need to be completed in this template are marked yellow.

Do you want to know more about the processor, controller and processing agreements? Please have a look at our website https://penrose.law/en/privacy-data-cookies/#data.

This template data processing agreement is provided by Penrose for information purposes. Penrose is a law firm in Amsterdam, specialized in corporate law, IP / IT law and employment law.

The model is periodically updated and published on www.penrose.law, as a result of which it may temporarily not reflect the latest legislative developments. Furthermore, this example is not an advice and no rights can be derived from it. If you have any questions, you can email us via info@penrose.law, or call us via +31(0)20-2400710.

DATA PROCESSING AGREEMENT (DPA)

THE UNDERSIGNED:

1. [●], a company statutory vested in ([●]) [●], having its principal place of business at [●] and registered with the Chamber of Commerce under number [●], hereby duly represented by [●], and hereinafter referred to as "**Processor**";

and

2. [●] a company statutory vested in ([●]) [●], having its principal place of business at [●] and registered with the Chamber of Commerce under number [●], hereby duly represented by [●], and hereinafter referred to as "**Controller**";

Controller and Processor are also individually referred to as "**Party**" and collectively as "**Parties**",

TAKING INTO CONSIDERATION THE FOLLOWING:

A. Processor and Controller have entered into an agreement (the "**Agreement**") based upon which Processor is providing certain services to Controller, whereby it may also process personal data under the control of Controller and to which Controller is considered to be 'data controller' and Processor is considered to be 'data processor' within the meaning of the General Data Protection Regulation (the "**GDPR**");

B. In view of article 28 paragraph 3 of the GDPR, this data processing agreement (the "**DPA**") stipulates the conditions for processing the personal data by Processor in relation to providing the services to Controller.

DECLARE TO HAVE AGREED AS FOLLOWS:

1. SUBJECT AND SCOPE

1.1. This DPA applies to the processing of personal data by Processor in the course of providing its services under the Agreement. In the event of discrepancies between provisions of this DPA and provisions of the Agreement, the provisions of this DPA shall prevail.

1.2. All definitions used in this DPA, such as 'personal data' and 'processing', will have the meaning given thereto under the GDPR.

1.3. Annex 1 (under A.) to this DPA contains an overview of the types of personal data and the categories of data subjects that are being processed and the purpose(s) for processing.

1.4. Any reference in this DPA to "written" is also meant to include "by electronic means" (e.g. email).

2. OBLIGATIONS OF PROCESSOR

2.1 Processor shall process the personal data solely upon instruction and on behalf of Controller. The processing of personal data shall be carried out in accordance with the written instructions of Controller and in compliance with the GDPR and any other applicable laws and regulations.

2.2 Processor shall not be permitted be use the personal data for other, own purposes.

2.3 Processor has implemented at least the technical and organizational security measures as outlined in Annex II of this DPA. In implementing the security measures, consideration has been given to the nature of the personal data, risks to be mitigated, the state of the art, and the costs of the security measures. This includes, among other things, that the personal data is protected against a security breach that leads or may lead to the destruction, loss, alteration, or unauthorized disclosure of or access to the personal data, whether accidental or unlawful (breach related to personal data).

2.4 Processor acknowledges that in order to safeguard an adequate level of security, additional ad-hoc security measures may be required. Processor undertakes to comply without delay with all requests from Controller to take additional security measures.

2.5 Upon request of Controller, Processor will provide assistance to Controller in the execution of data protection impact assessments (DPIA).

2.6 Processor shall not process the personal data to countries outside the European Economic Area (EEA) without prior, written consent of Controller. The transfer of personal data by the Processor to a third country or an international organization shall occur solely on the basis of written instructions from the Controller or to comply with a specific requirement under EU law or the national law to which the Processor is subject, and shall take place exclusively in accordance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

3. TERM AND TERMINATION

3.1 This DPA enters into force from the moment it is signed by all Parties and shall continue to be in force for the term as indicated in the Agreement, and in the absence thereof, for the duration of the services provided by Processor.

3.2 Neither Party can terminate this DPA for convenience.

3.3 Upon termination of the Agreement and/or upon first written request of the Controller, the Processor shall return or destroy, as to the Controller's sole discretion, all personal data without withholding any copies thereof, and direct any employees and/or sub-processors to do the same.

3.4 Upon first request of the Controller, the Processor shall confirm in writing the completion of the undertaking set forth in paragraph 3.3 in writing.

4. USE OF THIRD PARTIES/SUB-PROCESSORS

4.1 The Processor shall not appoint or engage any third parties (e.g. sub-processors) for the processing of personal data hereunder without the prior, written consent of Controller. Processor is currently using the third party sub-processors for the processing of the personal data of the Controller as listed in Annex I (under B.). Processor warrants that these approved sub-processors are bound by at least the same obligations regarding the protection of personal data as agreed under this DPA.

4.2 The Processor shall notify the Controller in writing at least 30 days in advance of any intended changes to that list by adding or replacing sub-processors, so that the Controller has sufficient time to raise objections to such changes before the engagement of the relevant sub-processor(s). The Processor shall provide the Controller with the information necessary for the latter to exercise its right to object.

4.3 At the request of the Controller, the Processor shall provide the Controller with a copy of its sub-processing agreement(s) and of any subsequent amendments thereto.

4.4 The Processor shall remain ultimately responsible and liable at all times for any damage or (detrimental) consequences resulting from the acts or omissions by sub-processors in relation to the processing of the personal data. Processor shall inform Controller of any breach by the sub-processor of its contractual obligations.

5. CONFIDENTIALITY

5.1 The Processor shall keep the personal data confidential and not directly or indirectly disclose the personal data to third parties unless explicitly permitted as stipulated in this DPA.

5.2 The Processor warrants that its employees and approved sub-processors are aware of the confidential nature of the personal data and bound to confidentiality obligations by their employment agreement, non-disclosure agreement or otherwise.

5.3 The confidentiality obligations hereunder will not apply, when:

a. the Controller has consented to the disclosure of personal data to third parties; or
b. the Processor has a legal obligation to make the personal data available to a third party, in which event the Processor shall immediately inform the Controller of such request.

6. DATA BREACH

6.1 The Processor shall inform Controller immediately – in any event within [36] hours – in writing after becoming aware of a (potential) breach, thereby including the following details:

a. the nature of the breach, including, where possible, the types of personal data and categories of data subjects involved;
b. date and time of becoming aware of the data breach;
c. the (potential/anticipated) consequences of the data breach;
d. the measures that have been taken or are proposed to address the data breach and/or to mitigate the possible adverse effects thereof;
e. the contact person with the Processor and its contact details for further correspondence regarding the breach.

6.2 A 'data breach' is considered to be: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of - or access to – the personal data transmitted, stored or otherwise processed, or any indication that such a breach will occur or has occured.

6.3 The Controller will remain responsible for assessing whether or not to notify the relevant data protection authority and/or data subject(s) of the data breach.

6.4 The Processor shall at all times offer its assistance to the Controller in relation to an investigation to the (possible) data breach and/or to the timely notification to the relevant data protection authority and, where required, to any data subject(s).

7. RIGHTS OF DATA SUBJECTS

7.1 The Processor shall provide full cooperation to enable the Controller to timely comply with any data subject requests for the execution of their statutory rights in accordance with the GDPR, more specifically, any requests to access, correct or delete the personal data, or to

limit the processing thereof (including the withdrawal of previously provided consent to the processing), and requests in connection with the right to data portability.

7.2 If the Processor receives (direct) requests from a data subject to exercise its rights (such as access, rectification, or deletion of personal data), the Processor shall forward these requests to the Controller. The Controller will handle these requests themselves, with the Processor being able to assist if necessary.

8. AUDIT

8.1 The Controller is entitled to execute an audit in order to verify the Processor's compliance with this DPA and the relevant provisions in the GDPR.

8.2 In view of executing the audit, the Processor shall:

a) grant the Controller and/or the auditor with all necessary access and make available all requested information, and provide all cooperation in order to effectuate the execution of the audit;

b) proactively inform the Controller about relevant changes in its organization or performance;

c) agree with all approved third party sub-processors that the Controller is entitled to exercise the audit right as referred to in this clause also in relation to those third party sub-processors.

8.3 The Controller and/or the auditor engaged by the Controller shall keep all information obtained during the audit secret, and only use the information to verify the Processor's compliance with the obligations under this DPA and the GDPR.

8.4 The costs for executing the audit will be borne by Controller, unless it follows from the audit that the Processor does not comply or has not complied with one or more obligations under this DPA or the GDPR. The Processor will bear its own costs associated with providing its assistance and cooperation to the audit.

8.5 When irregularities are found during the audit, the Processor shall prepare a remediation plan within a reasonable timeframe and coordinate this with the Controller. To the extent that the Controller makes direct recommendations to the Processor arising from the audit, the Processor guarantees to implement these within the reasonable timeframe as determined by the Controller.

9. LIABILITY AND INDEMNIFICATION

9.1 Regardless of any agreed liability clause applicable between the Parties under the Agreement, the Processor shall be liable in relation to the Controller for any damages or disadvantage - including any fines imposed by the data protection authority - suffered as a result of an act or failure to act by the Processor under this DPA and/or acting in breach with an obligation under the GDPR.

9.2 The Processor indemnifies and holds the Controller harmless from and against any claims, damage, costs and/or other disadvantage of third parties (including data subjects), which are directly or indirectly arising from or connected to any act or omission of the Processor and/or its sub-processors to act in accordance with this DPA and/or an obligation under the GDPR.

10. APPLICABLE LAW AND COMPETENT COURT

10.1 This DPA is exclusively governed by the laws of the Netherlands.

10.2 Any disputes between the Parties arising from or in connection with this DPA shall be referred to the competent court in the district where the Controller has its registered office.

IN WITNESS HEREOF, AGREED AND EXECUTED,

[●]	[●]
_____	_____
Name: [●]	Name: [●]
Date: [●]	Date: [●]

ANNEX 1 Description of the personal data processing

A. Data Processing

Categories of Data Subjects whose personal data is being processed

…

Types of personal data being processed

…

Nature of the personal data processing

…

Purpose(s) of the personal data processing on behalf of the Controller

…

B. Sub-processors

The Processors makes use of the following third party ('sub-processors'):

(Sub-)processors	Processing

ANNEX 2 Technical and Organizational measures

The technical and organizational measures must be described in concrete terms and not in general terms.

The description of the technical and organizational security measures taken by the Processor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the data processing, as well as the risks to the rights and freedoms of natural persons. Examples of potential data protection measures may include:

- measures regarding the pseudonymization and encryption of personal data;
- measures that permanently ensure the confidentiality, integrity, availability, and resilience of processing systems and services;
- measures that guarantee the ability to timely restore the availability of and access to personal data in the event of a physical or technical incident;
- processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for securing processing;
- measures for the identification and authorization of users;
- measures for the protection of data during transmission;
- measures for the protection of data during storage;
- measures to ensure the physical security of locations where personal data is processed;
- measures to ensure that incidents are recorded;
- measures to ensure the system configuration, including the default settings;
- measures for internal governance and management in the field of IT and IT security;
- measures for the certification/assurance of processes and products;
- measures to ensure data minimization;
- measures to ensure data quality;
- measures to ensure limited data retention;
- measures to ensure accountability;
- measures to enable data portability and ensure deletion.
- […]