Data Processor Agreement ISOPlanner B.V.

Parties

Name:
Address:
Chamber of Commerce number:
Represented by:
(hereinafter: "Controller");

ISOPlanner B.V., located at the Simon van der Stellaan 15 2803 EJ Gouda, The Netherlands and registered with the Chamber of Commerce under 87175932 and represented by Mr. van Duuren (hereinafter "Processor");

considering that:

- Controller and Processor have entered into an agreement on _____ (hereinafter "the Agreement"), for the purpose of providing a SaaS platform designed to help Controller streamline their journey toward ISO certification.
- Controller designates the purposes and means for the processing and to which the conditions specified herein apply;
- the specific personal data that will be processed and the security measures taken are described in Attachment A.
- Processor is willing to do so and is also willing to comply with the obligations regarding security and other aspects of the General Data Protection Regulation (hereinafter "GDPR"), insofar as this is within its control.

and agree on the following:

Article 1. Purposes of processing.

1.1 Processor undertakes to process personal data on behalf of Controller under the terms of this Data Processor Agreement. Processing will only take place within the scope of the Data Processor Agreement for the purpose of providing a Software as a Service (SaaS) service that provides a planning tool for implementing ISO standards (hereinafter, "the Service").

1.2 Processor shall not process the personal data for any purpose other than as determined by Controller.

Article 2. Obligations of Processor

2.1 With respect to the processing mentioned in Article 1, Processor shall ensure compliance with the conditions imposed under the GDPR on the processing of personal data by Processor.

2.2 Processor shall inform Controller, upon its request and within a reasonable time, of the measures taken by it regarding its obligations under this Data Processor Agreement.

2.3 The obligations of the Processor arising from this Data Processor Agreement also apply to those parties that process personal data under the authority of Processor.

Article 3. Transfer of personal data

3.1 Processor may process personal data in countries within the European Union. Controller additionally authorizes Processor to process personal data in countries outside the European Union, provided that it has been determined by the European Commission that this country

ensures an adequate level of protection or an EC Model Contract has been concluded by Processor with the relevant third party outside the European Union.

3.2 Processor shall not process personal data in countries outside the European Union that have not been determined by the European Commission to ensure an adequate level of protection or with which an EC Model Contract has been concluded, without the prior written consent of Controller. Processor may attach further conditions to this consent.

Article 4. Division of responsibility

4.1 Processor is solely responsible for the processing of the personal data under this Data Processor Agreement, in accordance with the instructions of Controller and under the express (ultimate) responsibility of Controller. For all other processing of personal data, including in any case but not limited to the collection of the personal data by Controller, processing for purposes not notified by Controller to Processor, processing by third parties and/or for other purposes, Processor is not responsible. Responsibility for these processing operations rests solely with Controller.

4.4 With respect to Processor's liability, the limitation of liability shall apply to this Data Processor Agreement as contained in Processor's general terms of service.

Article 5. Engaging third parties or subcontractors

5.1. Controller hereby authorizes Processor to use a third party in the processing of personal data, pursuant to this Data Processor Agreement, in compliance with applicable privacy laws.

5.2. At the request of Processor, Processor shall inform Controller as soon as possible about the third parties.

Article 6. Security

6.1 Processor shall endeavor to take appropriate technical and organizational measures with respect to the personal data processing against loss or against any form of unlawful processing (such as unauthorized access, impairment, modification or disclosure of the personal data).

6.2 Processor shall make every effort to ensure that the security meets a level that is not unreasonable, taking into account the sensitivity of the personal data and the costs associated with implementing security measures.

Article 7. Duty to report

7.1. In the event of a security breach and/or a data leak (which is defined as: a breach of the security of personal data that leads to a significant risk of serious adverse consequences, or has serious adverse consequences, for the protection of personal data), Processor, to the best of its ability, shall make every effort to inform Controller about this without delay or at the latest within forty-eight (48) hours, as a result of which Controller will assess whether or not to inform the supervisory authorities and/or data subjects. Processor shall make best efforts to make the information provided complete, correct and accurate.

7.2. Processor shall ensure compliance with any (statutory) reporting obligations. If required by law and/or regulations, Processor shall cooperate in informing the relevant authorities and any data subjects.

7.3. The duty to report includes, at a minimum, reporting the fact that a leak has occurred, as well as:

- the date the leak occurred (if no exact date is known: the period during which the leak occurred;
- what is the (alleged) cause of the leak);
- what is the (alleged) cause of the leak;
- the date and time when the leak became known to Processor or any third party or

subcontractor engaged by it;

- the number of individuals whose data was leaked (if an exact number is not known: the minimum and maximum number of individuals whose data was leaked);
- a description of the group of individuals whose data were leaked, including the type or types of personal data leaked;
- whether the data has been encrypted, hashed or otherwise made unintelligible or inaccessible to unauthorized persons;
- What measures are planned and/or have already been taken to plug the leak and to mitigate its effects;
- contact information for following up on the report.

Article 8. Rights of data subjects.

8.1. In the event that a data subject makes a request to Processor to exercise his/her legal rights , Processor shall forward the request to Controller and notify the data subject. Controller will then continue to handle the request independently. If it turns out that Controller requires assistance from Processor to fulfill a data subject's request, Processor may charge a fee for this.

Article 9. Duty of confidentiality

9.1. All personal data that Processor receives from Controller and/or collects itself in the context of this Data Processor Agreement is subject to a duty of confidentiality towards third parties.

9.2. This obligation of confidentiality does not apply to the extent that Controller has given express consent to provide the information to third parties or if the provision of the information to third parties is logically necessary given the nature of the assignment provided under the performance of this Data Processor Agreement, or if there is a legal obligation to provide the information to a third party.

Article 10. Audit

10.1. Controller shall have the right to have audits performed by an independent IT expert bound by confidentiality to verify compliance with all items in this Data Processor Agreement.

10.2. Such audit shall only take place after Controller has provided reasonable arguments to justify an audit. Such an audit shall be justified when similar audit reports show that Processor is not compliant with this Data Processor Agreement. The audit initiated by Controller shall take place only once a year.

10.3. Processor shall cooperate with the audit and make available all information reasonably relevant to the audit, including supporting data such as system logs within a reasonable period of time. Controller shall ensure that the audit causes the least possible business disruption to Processor's other operations.

10.4. The findings as a result of the audit conducted will be reviewed by the Parties in mutual consultation and, as a result, may or may not be implemented by either or both Parties jointly.

10.5. The costs for the audit shall be borne by Controller.

Article 11. Duration and termination

11.1 This Data Processor Agreement is entered into for the duration as stipulated in the Agreement between the Parties and in the absence thereof, in any case for the duration of the cooperation.

11.3 The parties may amend this Data Processor Agreement only by mutual written consent.

11.4 After termination of the Data Processor Agreement, Processor shall promptly destroy the personal data received from Controller, unless the Parties agree otherwise.

Article 12. Other provisions

12.1 The Data Processor Agreement and its performance shall be governed by Dutch law.

12.2. All disputes, which may arise between the Parties in connection with the Data Processing Agreement, shall be submitted to the competent court in the district of the court that also has jurisdiction to adjudicate in the context of the Agreement.

12.3 If one or more provisions of the Data Processing Agreement prove not to be legally valid, the remaining provisions of the Processing Agreement will remain in force.

12.4 If the privacy legislation changes, the Parties will cooperate to adapt this Data Processor Agreement in order to (continue to) comply with this legislation.

12.5. In case of conflict between different documents or their annexes, the following order of precedence shall apply:

a. the Agreement;
b. this Data Processor Agreement;
c. the general terms of service of Processor;
d. any additional conditions.

Thus agreed and signed,

Controller	Processor
_____/_____/_____	04___/_08__/ 2025_____
Date	Date
	Ivar van Duuren
_____	_____
Name	Name
	
_____	_____
Signature	Signature

Attachment A

Personal data

The following personal data will be processed:

User Data:

- Name (first name, last name)
- Email address
- Business email address
- Username

System-related Data:

- Login details
- Audit logs

Security Measures

We have implemented the following security measures:

Hosting & Infrastructure:

- Hosting on Microsoft Azure with ISO 27001 certification
- All data is stored within the EU
- Regular security updates and patches

Access Security:

- Multi-Factor Authentication (MFA)
- Role-based access control
- Strong password policies

Data Security:

- Encryption of data in transit and at rest
- Regular backups
- Privacy by design principles

Operational Security:

- Regular security audits
- Incident response procedures
- Monitoring and logging

These measures are regularly evaluated and updated as needed in accordance with our security policies.