Prindustry

Sub-Processor Agreement

Version September 2024

This Sub-Processor Agreement forms an integral part of the arrangements agreed upon by the Parties on the date of signing (hereinafter: "**the Agreement**").

General

In this Processing Agreement, the following terms are understood to mean:

- **General Terms and Conditions**: the General Terms and Conditions of the Processor, which apply without exception to every agreement between Processor, Controller, and Sub-Processor.
- **Processor**: Prindustry BV, located at Hendrik Figeeweg 1M-2 in Haarlem The Netherlands, registered with the Chamber of Commerce under number 53 55 12 30 and legally represented by Mr. Ramon van Wingerden.
- **Controller**: The natural or legal person who has instructed the Processor to perform Work, also referred to as the Controller.
- **Sub-Processor**: The natural or legal person who receives the assignment to perform Work from the Controller.
- **Data**: The personal data as described in Appendix 1.
- **Data subject**: The end customer as described in Appendix.
- **Agreement**: Any arrangement between the Processor, Controller, and Sub-Processor for the performance of Work by the Processor on behalf of the Client.
- **Work**: All work assigned, or performed by the Processor in any capacity. This is interpreted in the broadest sense and includes at least the tasks specified in the order confirmation.

Parties

The Contractor, hereinafter: "**Processor**"

and

The Client, hereinafter: "**Sub-Processor**"

considering that

- Processor, in the context of Agreements with its clients, being the Controller (hereinafter: "Controller") as defined in Article 4(7) of the General Data Protection Regulation (hereinafter: "GDPR"), receives personal data to process them as a Processor and wishes to engage a Sub-Processor for the processing of (part of) this personal data;
- Processor is recognized as a Processor under Article 4(8) GDPR;
- Where this agreement refers to personal data, it means personal data as defined in Article 4(1) GDPR;
- The Controller designates the purposes and means for the processing, and the Processor imposes these purposes and means on the Sub-Processor via this agreement;
- The Processor wishes to have certain forms of processing carried out by the Sub-Processor;
- The Sub-Processor is willing to do so and also agrees to handle the personal data carefully and comply with other security obligations and aspects of the GDPR;
- The Parties, in light of the requirement from Article 28(3) GDPR, wish to record their rights and obligations in writing through this Sub-Processor Agreement (hereinafter: "Sub-Processor Agreement");

have agreed as follows

Article 1. Purposes of processing

1.1 Sub-Processor undertakes to process personal data on behalf of the Processor under the terms of this Sub-Processor Agreement. Processing will only take place in the context of the Processor's activities to fulfill the assignment given by the Controller via the Prindustry platform and achieve the purposes agreed upon, as set out in the Agreement.

1.2 The personal data to be processed by Sub-Processor under the Agreement, and the categories of Data Subjects from whom these data are derived, are listed in Appendix 1. Sub-Processor will not process the personal data for any purpose other than as determined by the Processor. The Processor will inform Sub-Processor of the processing purposes, insofar as they are not already mentioned in this Sub-Processor Agreement.

1.3 The Sub-Processor does not make independent decisions about the processing of personal data. The authority over personal data provided to Sub-Processor under this Sub-Processor Agreement or other agreements between the parties, as well as over the data processed by Sub-Processor in that context, rests with the Processor.

Article 2. Sub-Processor's obligations

2.1 With regard to the processing referred to in Article 1, Sub-Processor will ensure compliance with the requirements imposed by the GDPR on the processing of personal data.

2.2 Sub-Processor will inform the Processor, upon request, about the measures it has taken concerning its obligations under this Sub-Processor Agreement and the GDPR.

2.3 The obligations of the Sub-Processor arising from this Sub-Processor Agreement also apply to those who process personal data under the authority or on behalf of the Sub-Processor, including but not limited to employees, in the broadest sense of the word.

2.4 Sub-Processor indemnifies the Processor against any claims and legal actions from third parties, including supervisory authorities such as the Dutch Data Protection Authority and Data Subjects, based on or arising from a breach of the Dutch Data Protection Act, the GDPR, and/or this Sub-Processor Agreement.

2.5 Sub-Processor will immediately notify the Processor if it believes that an instruction from the Processor or Controller conflicts with the laws referred to in paragraph 1.

Article 3. Transfer of personal data

3.1 Sub-Processor may process personal data in countries within the European Economic Area (hereinafter: "EEA"). Transfers to countries outside the EEA are not permitted without the prior written consent of the Processor. The Processor may attach additional conditions to this consent.

3.2 Sub-Processor will inform the Processor, upon request, in which country or countries the personal data are processed.

Article 4. Distribution of responsibility

4.1 The authorized processing will be carried out by Sub-Processor in a (semi-)automated environment.

4.2 Sub-Processor is responsible for processing personal data under this Sub-Processor Agreement, in accordance with the instructions of the Processor, and under the express (final) responsibility of the Controller. For all other processing of personal data, including but not limited to the collection of personal data by the Processor and Controller, processing for purposes not reported by the Processor to Sub-Processor, processing by third parties and/or for other purposes, Sub-Processor is not responsible. The responsibility for these processing operations rests solely with the Controller and/or Processor.

Article 5. Liability

5.1 The liability of the Processor for direct damage suffered by the Controller as a result of an attributable failure by the Processor to fulfill its obligations under the Agreement is described in Article A.8 of Prindustry's General Terms and Conditions.

Article 6. Engagement of third parties or subcontractors

6.1 Sub-Processor may engage a third party in the context of the Processing Agreement, provided that the same GDPR measures or Processing Agreement applies.

6.2 Sub-Processor will unconditionally ensure that these third parties assume the same obligations in writing as those agreed between the Processor and Sub-Processor. Sub-Processor guarantees compliance with these obligations by these third parties and is itself liable to the Processor for all damages caused by these third parties as if it had committed the error(s) itself.

Article 7. Security

7.1 Sub-Processor will take appropriate technical and organizational measures concerning the processing of personal data to prevent loss or any form of unlawful processing (such as unauthorized access, alteration, modification, or disclosure of the personal data). See Appendix 2.

7.2 Sub-Processor will ensure that security meets a level that is not unreasonable, considering the state of the art, the sensitivity of the personal data, and the costs of implementing the security measures.

7.3 Sub-Processor has at least taken the following measures:

- Logical access control using passwords;
- Physical access security measures;
- Automatic logging of all actions involving personal data;
- Encryption of digital files containing personal data;
- Organizational access security measures;
- Securing network connections via Secure Socket Layer (SSL) technology;
- Purpose-based access restrictions;
- Control of granted permissions;
- Measures to prevent the top 10 threats as formulated by OWASP.

7.4 Sub-Processor will always maintain an appropriate and up-to-date security policy that includes the technical and organizational security measures. Sub-Processor will provide the Processor with access to the security policy upon request.

Article 8. Reporting obligation

8.1 In the event of (or suspicion of) a data breach (defined as: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed), Sub-Processor will inform the Processor without delay, and in any case within twelve (12) hours, after which the Processor will assess whether to inform the Controller. Sub-Processor will provide the information as fully, correctly, and accurately as possible. The reporting obligation applies regardless of the impact of the breach.

8.2 If necessary, the Processor will cooperate in informing the Controller.

8.3 The reporting obligation at least includes the reporting of the fact that a breach has occurred, as well as:

- The date on which the breach occurred (if the exact date is not known: the period in which the breach occurred);
- The (suspected) cause of the breach;
- The (currently known and/or expected) consequence;

- The date and time the breach became known to Sub-Processor or a third party or subcontractor engaged by Sub-Processor;
- The number of individuals whose data was breached (if the exact number is not known: the minimum and maximum number of individuals whose data was breached);
- The probable consequences of the breach with respect to personal data (cf. Article 33(3)(c) GDPR);
- A description of the group of individuals whose data was breached, including the type(s) of personal data involved;
- Whether the data was encrypted, hashed, or otherwise rendered unintelligible or inaccessible to unauthorized persons;
- What measures have been taken and/or are being proposed to resolve the breach and limit the consequences of the breach;
- Contact details for follow-up on the report.

Article 9. Rights of Data Subjects

9.1 If a Data Subject submits a request to exercise their legal rights to Sub-Processor, Sub-Processor will forward the request to the Processor and notify the Data Subject. The Processor will then handle the request independently.

9.2 Sub-Processor will assist the Processor, where necessary, to enable the Data Subject to exercise their legal rights.

Article 10. Confidentiality obligation

10.1 All personal data received by Sub-Processor from Processor and/or collected by Sub-Processor in the context of this Processing Agreement is subject to a confidentiality obligation towards third parties. Sub-Processor will not use this information for any other purpose than for which it was obtained, even if it has been anonymized and cannot be traced back to Data Subjects.

10.2 This confidentiality obligation does not apply insofar as the Processor has given explicit permission to disclose the information to third parties if disclosing the information to third parties is logically necessary given the nature of the provided assignment and the execution of this Sub-Processor Agreement, or if there is a legal obligation to provide the information to a third party.

Article 11. Audit

11.1 Processor has the right to conduct audits or have audits conducted by an independent third party bound by confidentiality to verify compliance with all points of this Sub-Processor Agreement and related matters.

11.2 This audit may take place at least once a year and additionally in the event of a concrete suspicion of misuse of personal data.

11.3 Sub-Processor will cooperate with the audit and provide all relevant information for the audit, including supporting data such as system logs and employees, as soon as possible and within a reasonable period, which shall not exceed two weeks unless there is an urgent need for a shorter deadline.

11.4 The findings resulting from the audit will be jointly evaluated by the parties. If the audit provides grounds for this, Sub-Processor will implement adjustments as instructed by the Processor.

11.5 The reasonable costs of the audit will be borne by Sub-Processor if it is found that work has not been performed in accordance with the Sub-Processor Agreement and/or errors are found in the findings attributable to Sub-Processor. In all other cases, each party will bear its own costs for the audit.

11.6 Sub-Processor will assist Processor in carrying out a Data Protection Impact Assessment (hereinafter: 'DPIA') by the Controller, when necessary. This assistance may include providing the necessary information to Processor for the proper execution of the DPIA by the Controller.

Article 12. Duration and termination

12.1 This Sub-Processor Agreement is entered into for the duration specified in the Agreement between the Parties and, failing that, for the duration of the cooperation.
12.2 The Sub-Processor Agreement cannot be terminated prematurely.
12.3 The Parties may only amend this Sub-Processor Agreement with mutual written consent.
12.4 Upon termination of the Sub-Processor Agreement, Sub-Processor will promptly destroy the personal data received from Processor, in accordance with Article 28(3)(g), which stipulates that it is the Processor's choice as to what happens to the data unless the parties agree otherwise.
12.5 Sub-Processor will cooperate fully in adapting this Sub-Processor Agreement to comply with any new privacy legislation.

Article 13. Further provisions

13.1 The Sub-Processor Agreement and its implementation are governed by Dutch law.
13.2 Any disputes arising between the Parties in connection with the Sub-Processor Agreement will be submitted to the competent court in the district where the court dealing with the Agreement is located.
13.3 If one or more provisions of the Sub-Processor Agreement are found to be invalid, the Sub-Processor Agreement will remain in force for the remainder. The Parties will then consult to agree on provisions to replace the invalid provisions that are valid and as close as possible to the intent of the provisions being replaced.
13.4 If privacy laws change, the parties will cooperate to amend this Sub-Processor Agreement to ensure ongoing compliance with such laws.
13.5 In the event of conflicts between different documents or their appendices, the following hierarchy applies:
1. The Agreement;
2. This Sub-Processor Agreement;
3. The General Terms and Conditions of Processor;
4. Any additional conditions.

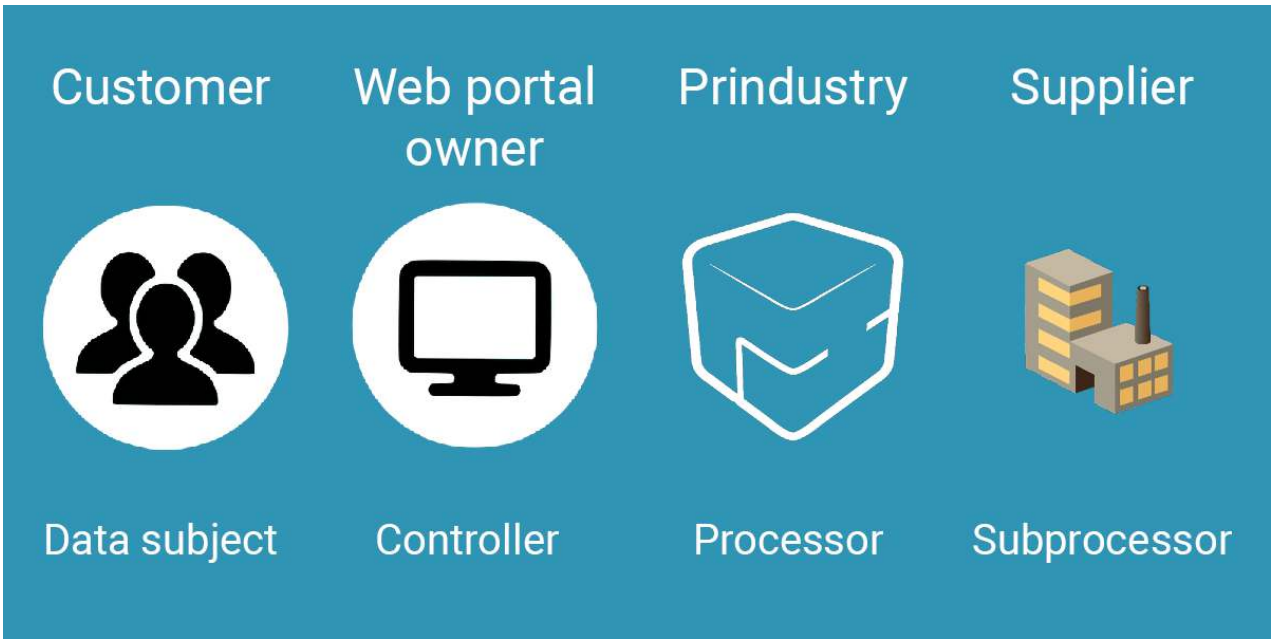
Thus agreed (digitally) by both parties from their registered addresses.

This document forms an integral part of a broader agreement and is therefore unsigned.

Prindustry

Appendix 1: Specification of Personal Data and Data Subjects

Roles in data processing by Prindustry



Data subject
The Data subjects whose personal data the Sub-Processor processes are the customers of the web portal – WhiteLabelShop or Brand Portal – owner. These include, for example, end customers of a WhiteLabelShop reseller or customers/employees who place (print) orders within a Brand Portal. All personal data of the Data subjects pertain to the data required to produce and ship the (print) order.

Controller
Personal data is processed on behalf of the Controller. The owner of the WhiteLabelShop or Brand Portal (webshop) is the Controller because they input or have others input the personal data and determine the purposes and means of processing.

Processor
Prindustry, as a software developer for its clients, is the Processor. Prindustry does not determine the purposes and means of processing personal data. Prindustry only stores the data and sends it via the platform.

The *Controllers* and *Processor* (Prindustry) also enter into a Data Processing Agreement concerning this relationship related to personal data (See the document 'Prindustry Processor Agreement,' available as an example on Prindustry's website).

Sub-Processor
When a WhiteLabelShop or Brand Portal owner uses connections to suppliers for the production of the web portal's (print) products, these suppliers become the Sub-Processors because they receive the personal data for a specific purpose, namely the production and shipping of an order. By signing the Sub-Processor Agreement, the suppliers indicate that they take appropriate measures to protect personal data.

This provides web portal owners with the assurance that personal data received for an order through the Prindustry platform is handled carefully. The Controllers can see in the backend of their web portal in the Prindustry Marketplace which suppliers have signed the Sub-Processor Agreement via the GDPR checkbox.

Personal data of Data subjects and Controllers

The Sub-Processor will process personal data of the Controller's Data Subjects via the Processor's (Prindustry's) platform under the Agreement.

Data end customers of web portal owner

The following personal data of end customers may be processed by the platform:

- First name
- Last name
- Gender
- Street name
- House number
- Postal code
- City
- Phone number
- Email address

Data web portal owner

The following data of web portal owners may be processed by the platform:

- First name
- Last name
- Company name
- Gender
- Street name
- House number
- Postal code
- City
- Phone number
- Email address

Prindustry

Appendix 2: Specification of security measures

Prindustry takes various technical and organizational measures concerning the processing of personal data to prevent loss or any form of unlawful processing (Article 7).

Technical measures

The main technical measures include servers within the EU and SSL certificates (also known as TLS certificates). All Prindustry servers are located within the EU and comply with GDPR regulations. All webshops and brand portals have a valid SSL certificate. By using an SSL certificate, all data is transmitted in an encrypted form. The SSL certificates are periodically validated. SSL/TLS certificates have an expiration date. For each SSL certificate, Prindustry keeps track of its validity (in the “Master List” available on Google Drive). Support keeps a calendar to track when a certificate needs to be replaced (to prevent the use of an expired certificate) and carries out the certificate replacement. When a certificate is replaced, the support staff records the new expiration date in the Master List and enters the new replacement date in the mentioned calendar. This falls under cryptographic management measures. Authentication data is stored in the database and in backups. Backups are stored in a protected environment in the data centre.
All internal processes at Prindustry are standardized to ensure a manageable organization, reliability, and efficiency.

Organizational measures

Organizational measures include, for example, keeping a Processing Register. This register lists which personal data is processed, for what purposes, and how this data is protected.
Prindustry is affiliated with the industry association ICTWaarborg. The ICTWaarborg certification is monitored and renewed annually. It stands for reliable ICT companies and provides partners with clarity and assurance.
Furthermore, Prindustry's information security management system (ISMS) has been ISO 27001 certified since 2021. The ISO 27001 standard indicates that Prindustry’s ISMS meets all requirements related to the continuous (further) development and secure operation of the Prindustry SaaS platform for webshops and brand portals. Prindustry’s ISMS is audited annually by an independent third party as part of this certification.