Processing Agreement

Version November 2022

This Processing Agreement is an integral part of the arrangements between the Parties as agreed on the day of signing the Agreement.

General

In this Processing Agreement the following terms have the following meanings:

- **General Terms and Conditions:** The General Terms and Conditions of the Processor, which apply in full to every agreement between the Processor and the Controller and of which General Terms and Conditions this Processing Agreement form an inseparable part.
- **Processor:** Prindustry BV, located at Hendrik Figeeweg 1M-2 in Haarlem, registered with the Chamber of Commerce under number 53 55 12 30 and legally represented by Mr. Ramon van Wingerden.
- **Controller:** The natural person or legal entity who has instructed the Processor to perform Work.
- **Data:** the personal data as described in Appendix 1.
- **Agreement:** Any agreement between the Controller and the Processor to perform Work by the Processor on behalf of the Client.
- **Work:** All work that has been commissioned or that are performed by the Processor on any other basis. The foregoing applies in the broadest sense of the word and in any case includes the work as stated in the order confirmation.

Parties

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

en

The Client, hereinafter: "**Controller**"

considering that:

- The Controller and the Processor have concluded an Agreement on the day of signing (hereinafter: ''the Agreement''), for the processing of personal data by the Processor as agreed in the Agreement, mainly in order to maintain and (continue to) develop the software platform and the web portal for the Controller;
- The Processor in the performance of the Agreement can be regarded as a Processor within the meaning of Article 4(8) of the General Data Protection Regulation (hereinafter: "GDPR");
- The Controller is regarded as a Controller within the meaning of Article 4(7) GDPR;
- Reference made in this Processing Agreement to personal data refers to personal data within the meaning of Article 4(1) of the GDPR;
- The Parties, also in view of the requirement in Article 28 (3) of the GDPR, wish to lay down their rights and obligations in writing by means of this Processor Agreement (hereinafter: "Processor Agreement");

have agreed as follows:

Article 1. Purposes of the processing

1.1 The Processor undertakes to process personal data on the instruction of the Controller, subject to the conditions of this Processing Agreement. Processing will only take place within the framework of the Processing Agreement and for the purpose of to maintain and further develop the software platform and the web portal for the Controller, and in order to achieve those objectives that have been laid down in the Agreement in mutual consultation.

1.2 The personal data that the Processor processes or will process within the framework of the Agreement and the categories of Data Subjects from whom the personal data originate are set out in Appendix 1. The Processor will refrain from using the personal data for any purpose other than that determined by the Controller. The Controller will inform the Processor of the purposes of the processing insofar as these are not already stated in this Processing Agreement.

1.3 The Processor has no control of the purposes and resources for the processing of personal data. The Processor will refrain from making any independent decisions with regard to the receipt and the use of the personal data, the provision thereof to third parties and the duration of storing personal data.

Article 2. Transfer of personal data

2.1 Processor may process personal data in countries within the European Economic Area (hereinafter: "EEA"). Transfer to countries outside the EEA is only permitted if this takes place on the basis of the prior written order / consent of the Controller, or if one of the appropriate safeguards within the meaning of the GDPR applies.

Article 3. Division of responsibility

3.1 The Processor will carry out the permitted processing activities within a computerized or semi-computerized environment.

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

3.3 The Controller guarantees that the content, the use and the assignment for the processing of the personal data as referred to in this Processing Agreement is not unlawful and does not infringe any right of third parties.

3.4 From the moment the GDPR comes into effect on 25 May 2018, the Parties will keep a register of the processing operations regulated under this Processing Agreement.

Article 4. Liability

4.1 Article A.8 of Prindustry's General Terms & Conditions describes Processor's liability for direct damages suffered by Processor as a result of an attributable breach by Processor of its obligations under the Agreement.

Article 5. Engagement of third parties or subcontractors

5.1 The Controller hereby gives the Processor permission to use a third party for the processing of personal data on the basis of this Processing Agreement, with due observance of the applicable privacy legislation.

5.2 At the request of the Controller, the Processor will inform the Controller as soon as possible about the third parties it has engaged. Controller has the right to object to any third parties engaged by Processor. If the Controller objects to third parties engaged by the Processor, the Parties will consult each other to find a solution.

5.3 The Processor will in any case ensure that these third parties assume the same obligations in writing as agreed between Controller and Processor. The Processor guarantees the correct compliance with these obligations by these third parties and, in the event of errors of these third parties, is itself liable to the Controller for all damage as if he had committed the error(s) himself.

Article 6. Security

6.1 Processor will endeavour to take appropriate technical and organizational measures with regard to the processing of personal data to be carried out, against loss or against any form of unlawful processing (such as unauthorized access, damage, modification or provision of the personal data). See Appendix 2.

6.2 Processor will make an effort to ensure that the security meets a level that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with security.

6.3 If it appears that a necessary security measure is missing, the Processor will ensure that the security meets a level that is not unreasonable in view of the state of the art, the sensitivity of the personal data and the costs associated with the security.

Article 7. Duty to report

7.1 In the event of a data leak (which means: a breach of security that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of, or unauthorized access to, forwarded, stored or otherwise processed data), the Processor will inform the Controller of this immediately or no later than within forty-eight (48) hours, on the basis of which the Controller will assess whether it will inform the supervisory authorities and / or data subjects or not. Processor makes every effort to ensure that the information provided is complete, correct and accurate.

7.2 Controller will ensure compliance with any (legal) reporting obligations. If required by law and / or regulations, Processor will cooperate in informing the relevant authorities and any parties involved.

7.3 The duty to report includes in any case reporting the fact that there has been a leak, as well as, insofar as it is known to the Processor:

- the date on which the leak occurred (if no exact date is known: the period within which the leak occurred);
- what is the (alleged) cause of the leak;
- the date and time when the leak became known to the Processor or a third party or subcontractor engaged by him;
- the number of persons whose data has been leaked (if no exact number is known: the minimum and maximum number of persons whose data has been leaked);
- a description of the group of persons whose data has been leaked, including the type or types of personal data that have been leaked;
- whether the data has been encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorized persons;
- what the proposed and / or already taken measures are to stop the leak and to limit the

consequences of the leak;
- contact details for the follow-up of the report.

Article 8. Rights of data subjects

8.1 In the event that a data subject submits a request to exercise his / her legal rights to the Processor, the Processor will forward the request to the Controller and inform the data subject thereof. The Controller will then handle the request independently. If it appears that the Controller needs help from the Processor to implement a request from a data subject, the Processor may charge costs for this.

Article 9. Duty of confidentiality

9.1 All personal data that the Processor receives from the Controller and / or collects itself in the context of this Processing Agreement is subject to a duty of confidentiality towards third parties. Processor will not use this information for a purpose other than that for which it has been obtained, unless it has been brought into such a form that it cannot be traced back to data subjects.

9.2 This duty of confidentiality does not apply insofar as the Controller has given explicit permission to provide the information to third parties, if the provision of the information to third parties is logically necessary in view of the nature of the assignment given and the implementation of this Processing Agreement, or if there is a there is a legal obligation to provide the information to a third party.

Article 10. Audit

10.1 The Controller has the right to have audits carried out by an independent ICT expert who is bound by confidentiality to check compliance with all points in this Processing Agreement.

10.2 This audit will only take place after the Controller has requested and assessed the similar audit reports available at the Processor and has submitted reasonable arguments that justify an audit initiated by the Controller. Such an audit is justified if the similar audit reports present at the Processor provide no or insufficient information about compliance with this Processing Agreement by the Processor. The audit initiated by the Controller takes place two weeks after prior announcement by the Controller, and no more than once a year.

10.3 Processor will cooperate with the audit and provide all information reasonably relevant to the audit, including supporting data such as system logs, and employees as timely as possible and within a reasonable period, whereby a period of no more than two weeks is reasonable unless an urgent interest opposes this. The Controller will ensure that the audit causes the least possible business disruptive effect on the other activities of the Processor.

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

10.5 The reasonable costs for the audit will be borne by the Controller, on the understanding that the costs for the third party to be hired will always be borne by the Controller.

10.6 The Processor will support the Controller in the performance of a Data Protection Impact Assessment (hereinafter: "DPIA") if the Processor is obliged to do so under the GDPR. This support can manifest itself, among other things, in the Processor making the necessary information available to the Controller for the correct execution of the DPIA.

Article 11. Duration and termination

11.1 This Processing Agreement has been entered into for the duration as determined in the Agreement between the Parties and, in the absence thereof, in any case for the duration of the collaboration.

11.2 The Processing Agreement cannot be terminated prematurely.
11.3 Parties may only amend this Processing Agreement with mutual written consent.
11.4 After termination of the Processing Agreement, the Processor will immediately destroy the personal data received from the Controller, unless the parties agree otherwise.

Article 12. Other conditions

12.1 The Processing Agreement and its implementation are governed by Dutch law.
12.2 All disputes that may arise between the Parties in connection with the Processing Agreement will be submitted to the competent court in the district of the court that is also competent to judge within the framework of the Agreement.
12.3 If one or more provisions of the Processing Agreement prove not to be legally valid, the Processing Agreement will remain in force for the rest. In that case, the parties will consult on the provisions that are not legally valid, in order to make a replacement arrangement that is legally valid and that matches the purport of the arrangement to be replaced as much as possible.
12.4 If the privacy legislation changes, the parties will cooperate to adjust this Processing Agreement in order to (continue to) comply with this legislation.
12.5 In the event of conflict between different documents or their appendices, the following order of precedence applies:

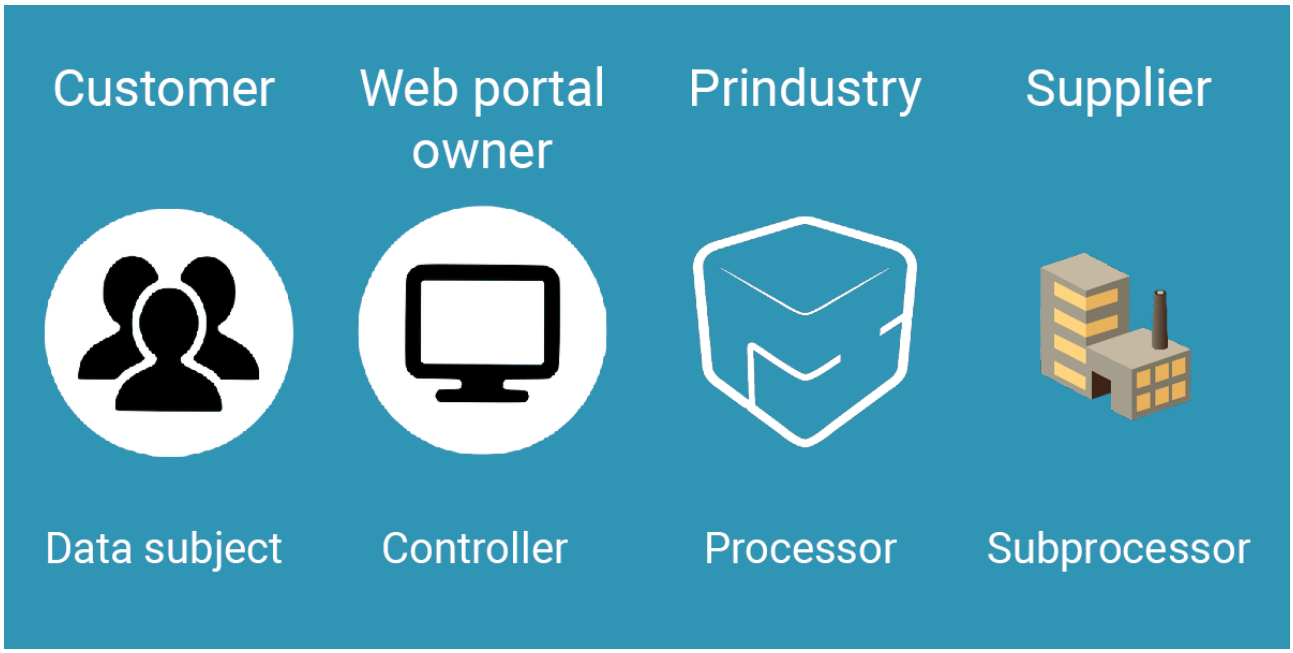
a. the Agreement; the Main Agreement, the contract;
b. this Processing Agreement;
c. the General Terms and Conditions of the Processor;
d. any additional conditions.

Thus agreed (digitally) by both parties from their business address

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

Appendix 1: Specification of personal data and data subjects

Roles data processing Prindustry



Data Subject
The intended Data Subjects of whom the Controller, Processor and Sub-Processor can process personal data are the (end) customers and / or employees of the WhiteLabelShop or Brand portal owner. It concerns their personal data that are processed through the platform of Processor Prindustry.

Controller
Personal data is processed on behalf of the Controller. The WhiteLabelShop or Brand portal (web portal) owner, the Prindustry customer, is the Controller, because this owner enters the personal data and determines the purpose and means.

Processor
As a software developer, Prindustry is the Processor for its customers, the web portal owners. Prindustry does not determine the purpose and means of processing the personal data. Prindustry merely stores the data and sends it via the platform.

Sub-Processor
When a web portal customer of Prindustry uses the connections to producers to manufacture the webshop products, these producers are the Sub-Processors, because they receive the personal data for a specific purpose, namely the production and sending of an order.
By signing a Sub-Processing Agreement, these producers indicate that they take appropriate measures to protect personal data. This gives Prindustry customers the assurance that they will handle the personal data they receive for an assignment through the Prindustry platform with care.
The Controllers can see in the backend in their web portal in the Prindustry Marketplace which Sub-Processors have signed the GDPR Sub-Processing Agreement by means of the green GDPR tick.

Personal Data of Data Subjects

The Controller, Processor and Sub-Processor process personal data of Data Subjects of the Controller through Prindustry's platform in the context of the Agreement. All categories of Data Subjects are listed in Prindustry's Processing Register.

Data Subjects: End Customers

The following personal data of end customers may go through the platform for processing:

- Company name
- Personal name
- Address
- House number
- Postal code
- Residency
- Telephone number
- E-mail address
- Bank account number
- Chamber of Commerce number

Webportal owner

- First name
- Surname
- Company name
- Gender
- Address
- House number
- Postal code
- Residency
- Telephone number
- E-mail address
- -IP address of webshop

Sub-Processors

The following Sub-Processors may receive personal data from end customers through the Prindustry platform for processing orders:

- Probo
- Control Media
- Print.com
- Inpromo
- Drukwerkdeal
- Oblé
- Saxoprint
- Siersema Vlaggen
- Eurovlag
- Ballondrukkerij
- Hofprint Etiketten
- Digi Promotions
- Zig Zag Forms

- PF Concept
- Gozi
- Exposure Systems
- Van As
- Kantoorstempels
- EPS Amsterdam
- De Prest
- Postermen
- Ecoprint

Prindustry provides all such partners with Sub-Processor Agreements for signature to ensure the security of personal data.

Appendix 2: Specification of security measures

Prindustry takes various technical and organizational measures with respect to the processing of personal data to be performed, against loss or against any form of unlawful processing (Article 6).

Technical measures

The main technical measures are servers within the EU and SSL certificates (aka: TLS certificates). All Prindustry servers are located within EU borders and comply with GDPR legislation. All web shops and brand portals have a valid SSL certificate. By using an SSL-certificate, all data will be sent encrypted. The SSL certificates are validated on a periodic basis. The SSL/TLS certificates all have an expiration date. For each SSL certificate Prindustry keeps track of the expiry date. Support keeps track of when which certificate needs to be replaced (to prevent an expired certificate from being used) and performs the replacement of the certificates. When a certificate is replaced, the support employee records the new expiration date in the Master list and includes the new replacement date in said diary. This falls under cryptographic management measures. Authentication credentials are 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 manageable organization, reliability and efficiency.
Further technical measures include antivirus software, secure passwords and their management in a password manager and two-factor authentication.

Organizational measures

Organizational measures include, for example, the maintenance of a Processing Register. This register states which personal data are processed, for what purposes and how these data are secured. Prindustry is a member of the ICT industry association ICTWaarborg. The ICTWaarborg certification is monitored and renewed on a yearly basis. It stands for reliable ICT companies, and provides clarity and security to partners. Prindustry is ISO 27001 certified as of 2021, the ISO standard for information security. The ISO 27001 certification indicates that Prindustry complies with all information security requirements for the continuous development and secure operation of the Prindustry SaaS platform for webshops and brand portals. This standard is audited every year.
Further organizational measures include limiting access to data (by authorization and authentication) and guidelines within the organization about processing personal data.

In Prindustry's Processing Register all technical and organizational measures per supplier can be found.