Data Processing Agreement PAYPRO - MERCHANT

Agreement for the protection of personal data.

Parties

1. Merchant registered with PayPro under number XXXXXX, with company details known to PayPro as recorded in the Agreement;
2. PayPro B.V., located in Groningen and registered in the trade register of the Chamber of Commerce under number 50398784, hereinafter referred to as “PayPro” and “Processor”.

Hereinafter referred to as “Merchant” and “Controller”, collectively referred to as “Parties”.

Considerations

1. This agreement applies to the relationship between the Parties where personal data processing takes place, effective from XXXXXX, hereinafter referred to as the “Data Processing Agreement”;
2. PayPro provides the Merchant with the Web Application based on the Agreement, through which the Merchant can use PayPro’s Payment Services, in the context of which PayPro processes Personal Data for the Merchant;
3. The Merchant is the controller within the meaning of the GDPR as the Merchant determines the purpose of the processing of personal data under the Agreement and controls the means used for this;
4. PayPro is the processor within the meaning of the GDPR as it processes Personal Data on behalf of and under the instructions of the Merchant based on the Agreement;
5. The Parties will handle the Personal Data processed under the Agreement carefully and in accordance with the GDPR and related applicable laws and regulations concerning the Processing of Personal Data;
6. The Parties will document their rights and obligations regarding the Processing of Personal Data of Data Subjects in this Data Processing Agreement in accordance with the GDPR and related applicable laws and regulations.

1. Definitions

- **Affiliates**: persons or organizations promoting third-party products and/or services through their own channels such as a website or social media.
- **Affiliate Link**: a link used by an Affiliate to direct internet users to the webshop, product, or service of a Merchant.
- **Customer**: the party entering into an agreement with the Merchant for the purchase of a product or service from the Merchant.
- **GDPR**: General Data Protection Regulation.
- **Payment Service**: the payment method provided by PayPro to the Merchant under the Agreement.
- **Data Subject**: an identified or identifiable natural person (Article 4(1) GDPR).
- **Agreement**: agreement for the acceptance of payments, the purchase of service modules, and/or sales support by Affiliates, as agreed between PayPro and the Merchant.
- **Personal Data**: any information relating to an identified or identifiable natural person (“the data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Article 4(1) GDPR).
- **Processing**: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data.

- **Web Application**: the online user account provided by PayPro to the Merchant, through which the Merchant can use the Payment Services.
- **Wwft**: Anti-Money Laundering and Anti-Terrorist Financing Act.

2. Subject

1. Under the Agreement, the Processor offers the use of the Web Application for the Controller. By using the Web Application, the Processor processes Personal Data of Customers.
2. The Processor will process Personal Data of Customers with great care and in accordance with the purposes of the processing and the instructions and provisions of this Data Processing Agreement.

3. Obligations of the Controller

1. The Controller will notify the Processor of any changes regarding the Processing and the possible consequences thereof in a timely manner, no later than 10 working days before the changes take effect.
2. The Controller guarantees the Processor that the assignment for the Processing of Personal Data is lawful and does not infringe on the rights of third parties.

4. Obligations of the Processor

1. The Processor will only process Personal Data if and to the extent necessary for the execution of the Agreement and will follow all reasonable instructions of the Controller.
2. The Processor will only transfer Personal Data to countries outside the European Economic Area with prior written consent from the Controller. The Controller may attach conditions to its consent.
3. The Processor ensures that its employees involved in the Processing of Personal Data comply with the provisions of this Data Processing Agreement. The employees of the Processor are bound by a confidentiality obligation.
4. The Processor will, upon the first request of the Controller, as soon as possible, hand over all Personal Data processed on behalf of the Controller to the Controller. The same applies to the request of the Controller to destroy the Personal Data, except for those Personal Data that the Processor is required to retain under applicable laws and regulations.
5. The Processor will take appropriate technical and organizational security measures to protect the Personal Data against loss and unlawful processing. These measures ensure, considering the state of the art and the costs of implementation, an appropriate level of security given the risks of the Processing and the nature of the data to be protected. The security measures taken are included in Appendix 2.
6. The Processor keeps a register of all categories of processing activities carried out on behalf of the Controller.
7. The Processor provides the Controller with full and timely cooperation to allow Data Subjects to access their personal data, have their personal data deleted or corrected, and/or demonstrate that these personal data have been deleted or corrected, or, if the Controller disputes the Data Subject's position, record that the Data Subject considers their personal data to be incorrect.
8. The Processor takes adequate internal control measures to comply with the obligations of this Data Processing Agreement and documents these in a way that makes it easy to verify compliance. Processing activities and incidents related to Personal Data are recorded in log files.
9. At the request of the Controller and if possible, the Processor cooperates with the encryption and pseudonymization of Personal Data. If this leads to higher costs for the Processor, the Controller will reimburse these costs.
10. The Processor provides the Controller with all information necessary to demonstrate compliance with the Data Processing Agreement and makes audits, including inspections, by the Controller or its authorized auditor possible. The Controller or its authorized auditor will be required to maintain confidentiality during the audits

and inspections and report the security measures in general terms. The costs of the investigation are borne by the Controller.

11. The content and scope of the assignment for Processing and the fee to be paid for it are in accordance with what is regulated in the Agreement.

5. Sub-Processor

1. The Processor may outsource the execution of the Data Processing Agreement in whole or in part to a Sub-Processor. By signing the Data Processing Agreement, the Controller gives permission to the Processor to outsource the Data Processing Agreement in whole or in part. The Sub-Processors are listed in Appendix 3. The Processor remains the point of contact and responsible for the compliance with the provisions of this Data Processing Agreement for the Controller at all times.

2. The Processor will impose the same obligations on its Sub-Processors, through an agreement, as those arising for the Processor from this Data Processing Agreement and ensure compliance by the Sub-Processors. The Processor is fully liable to the Controller for the consequences of outsourcing work to a Sub-Processor.

6. Provision of Personal Data

1. The Processor does not provide Personal Data to others than the Controller unless written permission has been given by the Controller to the Processor or the Processor is required to provide Personal Data under applicable laws and regulations. The Processor will confirm each provision in writing, stating the parties and/or persons involved, as far as legally permitted.

2. If the Processor is required to provide Personal Data to third parties under applicable laws and regulations, the Processor will verify the basis of the request and the identity of the requester, inform the Controller about this before the provision as far as legally permitted, limit the provision to what is legally required, enable the Controller to exercise the rights of the Controller and Data Subjects, and defend the interests of the Controller and Data Subjects.

7. Security

1. The Parties take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, so that the Processing complies with the requirements of the GDPR and related applicable laws and regulations concerning the Processing of Personal Data and the rights of Data Subjects are safeguarded. The technical and organizational measures taken by the Processor are included in Appendix 2.

2. The Parties will consider the processing risks, especially as a result of destruction, loss, alteration, unauthorized disclosure of, or access to transmitted, stored, or otherwise processed data, whether accidental or unlawful, when setting up the security of Personal Data of Data Subjects.

3. The Parties take measures to ensure that any natural person acting under the authority of the Controller or Processor who has access to Personal Data of Data Subjects processes these only on behalf of the Controller under the Agreement or under applicable laws and regulations.

8. Data Breaches

1. In the event of a Data Breach at the Processor, the Processor will report this as soon as the Processor becomes aware of the Data Breach, without unreasonable delay, no later than 24 hours after becoming aware, to the Controller, specifying the nature of the Data Breach, the (likely) consequences thereof, and the measures taken to remedy or mitigate the consequences as far as these matters are known at the time of the report.

9. Confidentiality

1. Personal Data processed on behalf of the Controller under the Agreement will be treated confidentially by the Processor. After the termination of this Data Processing Agreement1

10. Liability

1. The Processor is liable for damages suffered by the Controller resulting from non-compliance with, or violation of, the requirements of the GDPR and/or this Data Processing Agreement.

2. The Processor's liability under the preceding article is limited to the amount paid out by the Processor's liability insurance in the relevant case. In any case, and regardless of the coverage by the Processor's liability insurance, the Processor's liability is limited to €100,000 per incident, unless the damage is caused by intent or gross negligence of the Processor.

3. The Controller indemnifies the Processor against claims from third parties, particularly Data Subjects, and any resulting damages, based on non-compliance with the requirements of the GDPR and related laws and regulations regarding the protection of Personal Data and/or this Data Processing Agreement.

4. The Processor covers the risks mentioned in article 9.1 through adequate liability insurance.

Duration and Termination

1. The Data Processing Agreement enters into force on the day of signing by the Parties.

2. The Data Processing Agreement ends upon termination of the Agreement, regardless of the reason for termination.

3. Upon termination of the Data Processing Agreement, the Processor will transfer all Personal Data to the Controller or, at the express written request of the Controller, destroy the Personal Data held by the Processor. There will be no destruction of Personal Data that the Processor is required to retain under applicable laws and regulations for the Processor and/or its services.

4. After termination of the Data Processing Agreement, the obligations that by their nature are intended to continue after termination of the Data Processing Agreement will remain in effect.

Dissolution

1. If the Controller or Processor fails to comply with the Data Processing Agreement and this failure is not remedied after notice of default, the other party may dissolve the Agreement in whole or in part, without prejudice to the right to compensation.

Amendments and Supplements

1. If there are any amendments or supplements to this Data Processing Agreement, they will be agreed upon in writing between the Controller and Processor. These amendments and/or supplements will be included in an addendum to this Data Processing Agreement and will be binding from the moment the Parties expressly agree to the provisions of this addendum.

Appendix 1 – Processing Activities Regarding Customers of Merchant by PayPro

Under the Agreement, it is possible for the Merchant to process various Personal Data in the Web Application. Depending on the choices of the Merchant regarding which data are entered in the Web Application and the chosen payment method, different Personal Data may be processed in the Web Application. The following data are obtained from the Merchant for the execution of the Agreement by PayPro. When processing transactions, the transaction data are also shared with parties involved in transaction processing. These are the Acquirers with whom PayPro has an agreement. Additionally, the Merchant has the option to link the PayPro system with systems that are not part of PayPro's services. A link can be made with Magento, WooCommerce, and Zapier. By linking with (one of) these systems, these systems receive the Personal Data processed in the PayPro system. The exact data involved depends on the system used. The overview of processing shows which Personal Data can be processed by PayPro.

Finally, PayPro uses Affiliate cookies for its services to Merchants and Affiliates. These cookies can create a link between the Affiliate who directs the visitor to the Merchant's website and any payment that results from this. For this purpose, the visitor's IP address (which is anonymized) is stored. Based on this information, the Merchant can reward the Affiliate for their efforts by granting a commission to the Affiliate.

Retention Period of Customer Personal Data

- **Processing #1**: The data processed depends on the payment method used and the choices of the Merchant. These data are retained for five years after the termination of the business relationship with the Merchant for which the transaction was processed or for five years after the execution of the relevant transaction.

- **Processing #2**: This processing involves the IP address of the Customer when they view or pay for a product or service offered by a Merchant of PayPro, whose transaction is processed by PayPro, using an affiliate link placed by an Affiliate registered with PayPro. An Affiliate cookie is placed for this purpose. This means that the relevant IP address is linked to the relevant Affiliate link. The retention period for this is five years.

Purpose of Processing Customer Personal Data

- **Processing #1**: The processing of these data has two purposes:

    1. To comply with the Agreement. Under the Agreement between the payment service provider and PayPro, it is possible for PayPro to offset the PayPro balance of the payment service user with the amount of the purchase when the Customer reverses the payment. For this, purchase data are needed. Additionally, it is possible for the payment service user to initiate a refund using PayPro's services.

    2. Legal obligation. PayPro is required under Article 34 of the Wwft to record the data related to the transaction for the benefit of the payment service user in a way that these data are retrievable and the relevant transaction is reconstructable for five years after the time of reporting an unusual transaction.

- **Processing #2**: Under the Agreement between the payment service user and PayPro, PayPro makes its affiliate network available. As a reward for the promotional activities of an Affiliate, PayPro pays commissions.

Legal Basis for Processing Customer Personal Data

- **Processing #1**: The legal basis for purpose 1 is the execution of the agreement. The legal basis for purpose 2 is a legal obligation.

- **Processing #2**: Under Article 11.7a of the Telecommunications Act, consent from the end user, here read as the Customer, is required before data may be read or placed on their equipment such as computers, laptops, tablets, or phones. Under paragraph 3 sub b of the same article, consent is not required when these data are necessary for the execution of the service, provided this has no or minimal impact on the privacy of the data subject. Minister Henk Kamp of Economic Affairs informed the House of Representatives in May 2013 about a proposed amendment to the so-called cookie law, which is part of the Telecommunications Act, which is now in force. The minister indicated that he intends to amend the law so that explicit consent is no longer required for Affiliate cookies, in addition to functional and analytical cookies. This is because Affiliate cookies are not intended to collect information about the user, but about the Affiliate. Based on this information, it can be determined which Affiliate is entitled to the payment of a commission because their advertisement led to a sale. When information obtained through Affiliate cookies is used only for these purposes, it will have no or minimal impact on the privacy of the internet user, and this type of cookie falls under the exception. Under the agreement between the Merchant and PayPro, PayPro can process the IP address for matching a click on the Affiliate link with the transaction at the Merchant. A click essentially means the IP address from which the click was realized. This IP address is anonymized by PayPro and will have no or minimal impact on the privacy of the internet user. Additionally, the IP address is only used for the purpose of paying Affiliate commissions. Therefore, this processing falls under the aforementioned exception and is thus legally based on a legitimate interest.

Recipients of Customer Personal Data

- **Processing #1**: Depending on the payment method chosen by the Customer and the choices of the Merchant, personal data may be shared with the Acquirers with whom PayPro has an agreement. The interest of the receiving parties is the execution of the agreement they have with PayPro, namely the processing of the transaction. Additionally, data of Customers are shared with systems for which the Merchant creates a link with the Web Application. The possible links are Magento, WooCommerce, and Zapier. The personal data shared depend on the system linked to the Web Application.

- **Processing #2**: If a product or service of the Merchant is paid for through the promotional activities of an Affiliate, the purchase data are also visible in the account of the relevant Affiliate in the Web Application.

OVERVIEW OF PROCESSING REGARDING CUSTOMER

Tabel

Personal Data	Retention Period	Purpose	Legal Basis	Recipients
Name, Address, City, Phone NUmber, Email Address, IBAN, Card number	5 years after the termination of the business relationship or up to five years after the execution of the relevant transaction.	Service to the Merchant to perform any funds, etc.	Execution of the agreement.	Acquirers with whom PayPro has an agreement. The interest of the receiving parties is the execution of the agreement they have with PayPro, namely the processing of the transaction.
In case the Customer is a sole proprietorship or a VOF: Trade Name, Trade Address, KVK number, Vat Number	5 years after the termination of the business relationship or up to five years after the execution of the relevant transaction.	To retain transaction data related to the Merchant.	Legal obligation.	If an affiliate link is used, Affiliate to monitor the execution of Affiliate commissions.
IP address (Affiliate cookie)	1 year	Execution of Affiliate commissions	Legitimate interest	

The source of the Customer's data is the Merchant. The Merchant ensures that PayPro receives the data necessary for transaction processing.

Appendix 2 – Measures and Certifications of PayPro

Measures

1. The Processor maintains a policy document that explicitly addresses the measures taken by the Processor to secure the processing of data and to ensure the privacy of Data Subjects whose Personal Data are processed.
2. The tasks and responsibilities regarding the Processing of Personal Data of Data Subjects are clearly defined in an internal policy document.
3. The Processor's employees involved in the Processing of Personal Data are bound by a confidentiality obligation and, if applicable, have undergone screening prior to employment, through a certificate of conduct requested and verified by the Processor.
4. All employees of the Processor and, where applicable, hired personnel and external users are instructed on the organization's security policy and procedures, as relevant to their function. This also includes attention to the handling of Personal Data.

5. The Processor's equipment and IT facilities are physically protected against unauthorized access.
6. The Processor has an internal policy describing access for authorized users to the information systems and services they need to perform their tasks, to prevent unauthorized access to information systems.
7. When workspaces are unoccupied, they are locked separately to deny access to unauthorized persons.
8. The Processor has procedures for the acquisition, maintenance, and destruction of Personal Data.
9. Activities related to Personal Data are recorded in log files. This also applies to other relevant events, such as attempts to gain unauthorized access to personal data and disruptions that could lead to the corruption or loss of personal data.
10. The Processor has built security measures into the Web Application for adequate access control for both the Merchant and the Processor's employees.
11. The use of the Web Application is actively monitored and managed. Additionally, the Processor has a procedure to handle any data breaches, including informing the Controller.
12. The Controller reports data breaches that fall under a legal reporting obligation to the relevant supervisory authority (often the Data Protection Authority).

Certifications

The Processor's servers are managed at separate locations where the hosting providers have taken many security measures such as: camera surveillance, burglary protection, 2 independent surveillance services, dual authentication with RFID access cards and iris scanners, VEB certification level 4, ISO/IEC 27001, and NEN 7510 certificates. Additionally, the Processor is certified as a Collecting Payment Service Provider (hereinafter: "CPSP") and has obtained an IDEAL certificate issued by Currence IDEAL B.V. Currence is the owner and trademark holder of the IDEAL payment formula. To obtain this certificate, PayPro had to demonstrate compliance with the security requirements set by Currence. Currence supervises this. By obtaining this certificate, PayPro is allowed to offer IDEAL payments as a CPSP.

Appendix 3 – Sub-Processors

1. Currence IDEAL BV
2. Atos Worldline N.V./S.A.
3. PayPal Pte Ltd
4. AfterPay B.V.
5. Klarna BV
6. Bancontact Company NV
7. ABN AMRO Bank N.V.
8. Sofort AG