



Wero Privacy Policy

Bank-integrated app

1.0 Introduction.....	3
2.0 Who is responsible for processing your Personal Data?	3
3.0 How may we use your Personal Data?.....	4
4.0 Are you obligated to provide your Personal Data?.....	5
5.0 How we share your Personal Data (Recipients)?	5
6.0 How we keep your Personal Data inside the European economic area (EEA)?	6
7.0 How to exercise your rights?	6
8.0 Amendments	7
9.0 Contact.....	7

1.0 Introduction

This personal data protection policy (hereinafter the "**Policy**") specifically applies to the Wero digital wallet embedded in the mobile app of your bank or payment institution (hereinafter "**Wero Digital Wallet**") and describes how and to what extent your Personal Data are processed by EPI Company SE acting as controller when a user of the Wero Digital Wallet (hereinafter "**User**" or "**you**") uses the Wero Digital Wallet. The Policy supplements the terms & conditions of your bank or payment institution (hereinafter the "**Bank**").

The Wero Digital Wallet is an e-payment application embedded in the mobile banking application distributed by your Bank. Although for most of the processing activities carried out for the operation of the Wero Digital Wallet, the controller is your Bank, certain processing activities described in this Policy are performed by EPI Company SE acting as controller. EPI Company SE (hereinafter referred to as "**EPI**", "**we**", "**us**", "**our**"), a company registered in Belgium with the Crossroads Bank for Enterprises under the number 0755.811.726, with the registered headquarters located at: at De Lignestraat 13, 1000 Brussels, Belgium.

As the protection of Personal Data is our major concern, WE are committed to Processing Personal Data with the utmost transparency and in compliance with applicable European and national data protection regulations (hereinafter the "**Applicable Regulations**"), particularly Regulation (EU) 2016/679 of April 27, 2016 (hereinafter the "**GDPR**") and the Belgian law of 30 July 2018 on the protection of natural persons regarding the Processing of Personal Data.

This Policy outlines how we, as the Controller, handle YOUR Personal Data in line with the Applicable Regulations and explains how YOU can exercise YOUR rights under these regulations. To ensure that WE Process YOUR Personal Data in accordance with Applicable Regulations and this Policy and to answer any questions YOU may have regarding EPI's Processing of YOUR Personal Data, WE have appointed a Data Protection Officer who can be contacted by email at dpo@epicompany.eu.

The terms "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Recipient**" and "**Data Subject**" used in this Policy refer to the terms defined in Article 4 of the GDPR.

2.0 Who is responsible for processing your Personal Data?

EPI acts as the Controller for the Processing of Personal Data under this Policy. This Policy specifically covers the processing of Personal Data by EPI as controller for the operation of the Wero Digital Wallet.

This Policy does not cover the following:

- **EPI and Wero Websites:** The processing of Personal Data for the operation of the EPI and Wero websites is governed by separate privacy statements dedicated to those websites.
- **Wero App:** The processing of Personal Data for the operation of the Wero App is governed by separate privacy statements accessible from this app.
- **Processing as a Processor:** In most cases, EPI processes Personal Data for the functioning of the Wero Digital Wallet on behalf of and under the instructions of your Bank. In this context, your Bank acts as a separate Controller and EPI as Processor. For the processing carried out by EPI as a processor for your Bank in relation to the operation of the Wero Digital Wallet, please refer to your bank's privacy statement.

3.0 How may we use your Personal Data?

As part of the Processing operations that we carry out as controller for the functioning of the Wero Digital Wallet, we process the following categories of Personal Data:

Purpose	Legal Basis	Categories of Personal Data processed	Retention period
Monitoring of the P2P transactions to ensure that a P2P transaction is not carried out by a professional	Legitimate interest (Art. 6.1.f of GDPR)	Pro tag Number of transactions per day/month Cumulated amount of the transactions per day/month	Until deactivation of the Wero Digital Wallet
Fraud prevention and scoring related to e/m-commerce transactions, disputes and refunds	Legitimate interest (Art. 6.1.f of GDPR)	Information about you (name and surname, date of birth) Data related to the transaction (amount, creation and expiry dates of the payment request or payment transaction) Data related to the dispute (see below) Data related to your Wero Digital Wallet (unique identifier, app name and onboarding timestamp) Telemetric data related to your mobile device* (model name and model number, screen resolution, cellular provider, location, time zone indicator, Id, operating system, choice of language, time, IP address, client IP address, user agent, client user agent) Fraud data (fraud score, primary risk vector for the fraud score)	Maximum twenty-four (24) months from the date of collection.
Fraud notification and reporting to YOUR Bank and the bank of the counterpart	Legitimate interest (Art. 6.1.f of GDPR)	Data related to the transaction (transaction identifier, amount, currency, consent token, wallet identifier) Fraud category	Maximum five (5) years from the fraud notification

Improvement of the fraud scoring engine	Legitimate interest (Art. 6.1.f of GDPR)	Anonymized data used for the fraud prevention Data related to fraudulent transactions (unique identifier, amount, payee's name, fraud category)	Maximum twenty-four (24) months from the date of collection. Maximum five (5) years for fraudulent transactions
Management and arbitration of commercial dispute resolution on the Wero dispute resolution platform (performance of a contract – art. 6.1.b of GDPR)		Data related to the transaction (amount, timestamp) Data related to the merchant Data related to the basket items (name, quantity, price)** Shipping and billing address** Information about the dispute (reason for the dispute, message from the consumer)	Maximum five (5) years from the dispute resolution

*Depending on your Bank.

** Depending on the bank of the merchant

In addition, if WE use YOUR Personal Data for purposes other than those mentioned above, WE will notify YOU of these purposes before using YOUR Personal Data and obtain YOUR consent where necessary.

4.0 Are you obligated to provide your Personal Data?

We need some of your Personal Data for the performance of our contract (the terms & conditions of YOUR Bank on the Wero dispute resolution platform) with you. If YOU do not provide us with your Personal Data, certain functionalities of our app cannot be used, for example, YOU cannot register without providing us the identity information set out above, or we might not be able to fulfil our contract with YOU. Some of YOUR Personal Data are collected directly by EPI and others provided to EPI by YOUR Bank.

5.0 How we share your Personal Data (Recipients)?

Only duly authorized staff members of EPI and its affiliates may have access to YOUR Personal Data, and only on a "need to know" basis. These internal Recipients are subject to strict security and confidentiality obligations.

Furthermore, WE may only share YOUR Personal Data to the following external Recipients for the purposes set out in section 3 of this Policy:

- External service providers and suppliers who perform Services on our behalf as Processors and only in accordance with OUR documented instructions, including our service providers for data hosting, analytics, application programming interfaces, crash reporting, security monitoring and fraud scoring and detection;

- Financial institutions, including YOUR Bank and merchants involved in the transaction, in order to process payment transactions and perform other activities that YOU request;
- Law enforcement agencies, or competent administrative or judicial authorities, either to comply with a legal, regulatory, judicial or administrative obligation (for example to report an illegal activity), or in the context of litigation to protect ourselves against any infringement of OUR rights;
- Potential or future buyers in the context of a potential corporate transaction; and
- External professional advisors (e.g. auditors, lawyers or consultants of EPI).

6.0 How we keep your Personal Data inside the European economic area (EEA)?

EPI endeavours not to transfer any Personal Data outside the European Economic Area (EEA). However, if YOU request it or as part of a transaction with someone outside the EEA (such as sending or receiving funds), WE may need to transfer YOUR data internationally.

Where applicable, the transfer of Personal Data outside the EEA is governed by the applicable regulations and is subject to strict conditions to guarantee Personal Data protection (and in particular the use of the European Commission's standard contractual clauses, of which a copy can be obtained by contacting OUR data protection officer where the transfer does not rely (i) on a valid adequacy decision of the European Commission or (ii) an exception under Art. 49 GDPR like necessary for the performance of a contract).

7.0 How to exercise your rights?

As a Data Subject, YOU have various rights regarding YOUR Personal Data that WE Process as a Controller. YOU can exercise these rights at any time under the conditions set forth in the Applicable Regulations. Here's a summary of YOUR key rights:

- **Right of access:** YOU may request confirmation from EPI as to whether or not Personal Data concerning YOU is being Processed and, if so, YOU may request access to YOUR Personal Data;
- **Right of rectification:** If YOUR Personal Data is incorrect, incomplete or not up to date, YOU can ask EPI to correct, update or complete it;
- **Right to erasure:** in certain situations provided for in Article 17 of the GDPR, YOU may ask EPI to delete YOUR Personal Data;
- **Right to restriction:** in certain situations provided for in Article 18 of the GDPR, YOU may ask EPI to limit the Processing of YOUR Personal Data to certain purposes and under several conditions;
- **Right to object:** where Processing is carried out in accordance with a legitimate interest of EPI, YOU can object to this Processing unless WE have compelling legitimate grounds to continue.
- **Right to data portability:** where the Personal Data is necessary for the performance of a contract with YOU or is Processed on the basis of YOUR consent, YOU may request EPI to communicate YOUR Personal Data to YOU in a structured, commonly used and machine-readable format; and/or to transmit it to another Controller;
- **Withdrawal of YOUR consent** (if applicable): where YOUR Personal Data is Processed on the basis of YOUR consent, YOU may withdraw this consent at any time;
- **Right to define post-mortem directives:** where allowed by national laws such as French law, YOU can set directives for how YOUR Personal Data should be handled after YOUR death.

YOU can exercise YOUR rights by sending an e-mail to OUR data protection officer at the following address: dpo@epicompany.eu. WE may ask for proof of identity if there is any doubt about YOUR identity.

If YOU believe YOUR rights have been violated, YOU have the right to file a complaint with a supervisory authority. The supervisory authorities competent for US are in particular the Belgian data protection authority and, if YOU reside in the EU, the EU data protection authority in YOUR country of residence, YOUR place of work or the place where an alleged infringement took place, which YOU can find using the contact options set out here: https://edpb.europa.eu/about-edpb/about-edpb/members_en. A list of the German supervisory authorities can be found here: <https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>.

We are committed to addressing your concerns and ensuring your rights are protected.

8.0 Amendments

This Policy will be updated from time to time to reflect regulatory changes and/or technological and Services developments and implementation into the Wero App. Any changes will be effective immediately upon posting of the updated Policy on OUR website and in the Wero App. WE encourage YOU to review this Policy periodically to stay informed about how WE are protecting YOUR information.

If WE make material changes to this Policy, WE will notify YOU by email or by posting a notice on OUR website prior to the effective date of the changes. Except where consent is required by the Applicable Regulations, YOUR continued use of OUR Services following the posting of changes constitutes YOUR acceptance of such changes.

9.0 Contact

9.1 EPI

If YOU have any questions, comments or concerns regarding the Policy and/or practices to protect YOUR data, please contact EPI through the following contact details:

Email: dpo@epicompany.eu

Address: De Lignestraat 13, 1000 Brussels, Belgium

9.2 Data Protection Officer

The data protection officer of EPI can be contacted through the following contact details:

Email: dpo@epicompany.eu

Address: De Lignestraat 13, 1000 Brussels, Belgium

Last updated: 30/06/2025