Wero App Privacy Policy

1.0 Introduction

This personal data protection policy (hereinafter the "**Policy**") specifically applies to the Wero App and describes how and to what extent your Personal Data are processed by EPI Company SE when a user of the Wero App (hereinafter "**User**" or "**you**") installs, activates, and uses the Wero App. The Policy supplements the Wero General Terms & Conditions.

The Wero App is a mobile e-payment application owned and operated by 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 is responsible for processing Personal Data as the Controller under this Policy. This Policy specifically covers the processing of Personal Data by EPI for the operation of the Wero App.

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.
- **Processing as a Processor**: EPI processes Personal Data for the processing of payment transactions and strong customer authentication on behalf of and under the instructions of your Eligible ASPSP (as defined in the Wero General Terms & Conditions). In this context, the Eligible ASPSP acts as a separate Controller and EPI as Processor. Please refer to their privacy statement for details on how your Personal Data is processed in these situations. However, for Deutsche Bank customers, EPI acts as a Controller, in accordance with the German version of the Policy, which is binding in this context.

3.0 How may we use your Personal Data?

As part of the Processing operations that we carry out, we process the following categories of Personal Data:

Purpose (and legal Basis)	Categories of Data processed	Retention period

Wero App enrollment & provisioning (performance of a contract – art. 6.1.b of GDPR)	Information about your payment source (account holder name, type of payment account, technical identifier of the payment source) Acceptance of our terms and conditions, with time of acceptance	Duration of the contract (the Wero General Terms & Conditions)
Issuing and confirmation of a payment request (performance of a contract – art. 6.1.b of GDPR)	Account holder name, amount, status, timestamp, message of P2P request, technical identifiers related to the payment source, the Wero App and the P2P request	13 months after the execution of the transaction
Initiation and confirmation of a P2P Payment (performance of a contract – art. 6.1.b of GDPR)	Account holder name, amount, status, timestamp, message of P2P payment, masked IBAN, technical identifiers related to the payment source, the Wero App and the P2P payment	13 months after the execution of the transaction
Initiation and confirmation of a commercial transaction (performance of a contract – art. 6.1.b of GDPR)	Legal name of the Acceptor (as defined in the Wero General Terms & Conditions), timestamp of creation, timestamp of expiry, transaction type and transaction parameters, date of birth, shipping address, masked IBAN	13 months after the execution of the transaction
Strong customer authentication for access to the wallet (Legal obligation - art 6.1.c of GDPR)	Authentication token, technical ID, externalId, 'pro' flag, Wallet id, walletName, hostModel, appId, appName.	13 months after the execution of the transaction
Displaying of the payee name (truncated) to the payer for prevention of fraud and errors (legitimate interest – art. 6.1.f of GDPR)	Name and surname	Duration of the contract (the Wero General Terms & Conditions)
Displaying your account information (performance of a contract – art. 6.1.b of GDPR)	Balance and transaction history of your payment account	Duration of the contract (the Wero General Terms & Conditions)
Fraud prevention and scoring related to transactions, including data anonymization to improve the fraud scoring engine (legitimate interest – art. 6.1.f of GDPR)	Information about your payment source (account holder name, technical identifier of the payment source, 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 your Wero App (unique identifier and app name) 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)	Maximum twenty-four (24) months from the date of collection. Maximum five (5) years for proven fraud

	Fraud data (fraud score, primary risk vector for the fraud score)	
Handling any requests you may make to our user service department and to notify you about changes to the Wero App or any other aspects connected to the Wero (legitimate interest – art. 6.1.f of GDPR)	The name(s), (e-mail) addresses and phone number(s) mentioned in your messages to us, the content of any message sent to us, any other information you chose to provide to us upon our request, such as proof of your identity	Duration needed to manage your request
Management and resolution of disputes regarding unauthorized or improperly executed transactions, as well as the handling of any other claims by payment service users (PSUs), in strict adherence to Article 101 of the Payment Services Directive 2 (PSD2) (legal obligation - art 6.1.c of GDPR)	Any data needed to manage the reports, complaints and claims including the transaction data	Five (5) years from the reporting, complaint or claim
Management of any pre-litigation and dispute procedures, in order to defend our rights (legitimate interest – art. 6.1.f of GDPR)	Any necessary data related to the pre-litigation and dispute	Duration of the dispute and any statute of limitations/forclosure period
Compliance with our legal obligations including Know your Customers (KYC), Anti-Money Laundering and the financing of terrorism, anti-corruption and economic sanctions, others laws or regulations applicable to the financial sector (task carried out in the public interest- art 6.1.e of GDPR)	Information provided by your Eligible ASPSP: external Id, name, date of birth, place of birth, location of residence. We may collect additional data directly from you where required by law.	Period of retention in accordance with legal and regulatory obligations (10 years for Anti-Money Laundering)
Crash reporting, analytics and security of the Wero Standalone App (legitimate interest – art. 6.1.f of GDPR)	Battery status, internet connection, network connection, app's current view, steps the user performed, view hierarchy when a bug is reported, full stack trace of the error, User IP address, Date and time of the request, Page Title, Page URL, Referrer URL, Screen resolution being used, Time in local user's timezone, Files that were clicked and downloaded, Links to an outside domain that were clicked, Pages generation time, Accept-Language header, User-Agent header.	1 year from the collection

For the avoidance of doubt, EPI does not collect nor process any of your special categories of Personal Data when you choose to enable the use of your mobile device Biometric ID (such as your fingerprint or face scan), to authenticate your payments in the Wero App.

4.0 Are you obligated to provide your Personal Data?

We need some of your Personal Data to comply with our legal obligations or for the performance of our contract (the Wero General Terms & Conditions) 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.

5.0 How we share your Personal Data (Recipients)?

Only duly authorized staff members of EPI and its affiliates are likely to 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 only communicate your Personal Data to the following External Recipients:

- 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 and fraud scoring;
- Financial institutions, including your Eligible ASPSP (as defined in the Wero General Terms & Conditions) and merchants involve in the transaction, in order to process payment transactions and perform other activities that you request;
- Law enforcement agencies, or competent administrative or judicial authority, 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.

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).

7.0 How we protect and secure your Personal Data?

At EPI, the security of your Personal Data is our priority. We take several steps to ensure that your data remains secure and confidential. Here’s how we protect your Personal Data:

- Comprehensive Security Measures: We implement a range of technical, administrative, and organizational measures designed to protect our information systems and your Personal Data from unauthorized access, alteration, disclosure, or destruction.
- Encryption: We use advanced encryption technologies to safeguard your Personal Data, particularly during transmission, to prevent unauthorized access.
- Confidentiality Protocols: Our team is trained and regularly updated on best practices for maintaining data confidentiality and security.

By using these methods, we strive to protect your Personal Data and maintain its integrity at all times.

8.0 How to exercise your rights?

As a Data Subject, you have various rights regarding your Personal Data that we process as 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 situation provided for in Article 17 of the GDPR, you may ask EPI to delete your Personal Data;
- **Right to restriction**: in certain situation 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, 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, which you can find using the contact options set out here: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

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

9.0 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 Regulation, your continued use of our services following the posting of changes constitutes your acceptance of such changes.

Last updated: January, 15th 2025.