Wero App Privacy Policy & Cookie notice

1.0 Introduction

This Personal Data protection policy & Cookie notice (hereinafter the "**Policy**") specifically applies to the Wero App and describes how and to what extent your Personal Data are Processed as well as to how and to which extend cookies are used by EPI Company SE when a user of the Wero App (hereinafter "**USER**", "**YOU**" or "**YOUR**") installs, activates, and uses the Wero App. The Policy supplements the Wero General Terms & Conditions. The terms "Acceptor", "Account", "Device", "Eligible ASPSPs", "EPI Scheme", "Open Banking ASPSP", "Open Banking Eligible Jurisdiction", "ASPSP", "P2P Transactions", "Services", "Strong Customer Authentication", "USER", "Wero App", and "Wero Transaction" used in this Policy have the same meaning as that given to them in the Wero General Terms & Conditions accessible by clicking HERE.

The Wero App is a mobile e-payment application owned and operated by EPI Company SE (hereinafter referred to as "**EPI**", "**WE**", "**US**", or "**OUR**"), a company registered in Belgium with the Crossroads Bank for Enterprises under the number 0755.811.726, with the refgistered headquarters located 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**", "**Process(ing)**", "**Controller**", "**Processor**", "**Recipient**" and "**Data Subject**" used in this Policy refer to the terms defined in Article 4 of the GDPR.

When using the Wero App, Personal Data may be Processed by means of cookies and similar technologies. More information on the use of these technologies can be found in our Cookie Notice under clause 8.

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 for the operation of the Wero App.

This Policy does not cover the following:

- **Processing as a Processor for ASPSPs:** EPI Processes Personal Data for the processing of Wero Transactions and Strong Customer Authentication carried out in this respect on behalf of and under the instructions of YOUR ASPSP. In this context, the ASPSP acts as a separate Controller and EPI as Processor. Please refer to the ASPSP's privacy statement for details on how YOUR Personal Data is Processed in these situations. **However, for USERS who are Deutsche Bank customers, EPI acts as a Controller in this context in accordance with Appendix 1 of this Policy.**
- **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 e-commerce bank selector**: The Processing of Personal Data for the operation of the Wero e-commerce bank selector is governed by separate privacy statements.

3.0 How may WE use YOUR Personal Data?

As part of the Processing operations that WE carry out as a Controller, WE Process the following categories of Personal Data, only for the purpose described below. For each purpose, the relevant legal basis is mentioned.

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
Wero App enrolment & provisioning	Performance of a contract (Art. 6.1.b of GDPR)	Information about YOUR payment source (account holder name, type of Account, technical identifier of the payment source) Acceptance of OUR Wero General Terms & Conditions, with time of acceptance	Duration of the contract (see section 13 of the Wero General Terms & Conditions)
Issuing and confirmation of a payment request for P2P Transaction (The term "P2P Transaction" refers to the term as defined in section 2 of the Wero General Terms & Conditions.)	Performance of a contract (Art. 6.1.b of GDPR)	Identification data (name and surname); contact data (phone number or email); technical identifiers related to the payment means and Wero App; P2P request data (amount, title, message, payment reference, timestamps, expiry date, status); reachability data (proxy identifiers or hash)	13 months after the execution of the transaction
Initiation and confirmation of a Wero Transaction	Performance of a contract (Art. 6.1.b of GDPR)	Identification data (name and surname); contact data (payee's phone number or email); technical identifiers related to the payment means and Wero App; P2P Transaction data (amount, timestamps, message, status, reference); reconciliation and reporting data	13 months after the execution of the transaction
Commercial transactions (Remote E/M-commerce transaction and point of sale Wero Transaction)	Performance of a contract (Art. 6.1.b of GDPR)	Transaction data (amount, timestamps, reference, payment status, capture and authorisation details); consent data; beneficiary data; consumer and wallet data; reconciliation and reporting data	13 months after the execution of the transaction
Strong customer authentication for access to the Wero App	Legal obligation under Art. 47 of the Belgian Payment and E-money Institutions Act of 11 March 2018	Authentication token, technical ID, external Id, 'pro' flag, Wallet id,	13 months after the execution of the transaction

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
	(implementing art. 94, 97, par 1 j. 4 Payment Services Directive 2) (Art 6.1.c of GDPR)[1]	walletName, hostModel, appId, appName.	
Displaying of the payee name (truncated) to the payer for prevention of fraud and errors	Legal obligation under Article 5c(1)(d) of Regulation (EU) No 260/2012 (SEPA) (Art. 6.1.c of GDPR)	Name and surname	Duration of the contract (see section 13 of 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 Account	Duration of the contract (see section 13 of the Wero General Terms & Conditions)
Fraud prevention and scoring related to transactions, including data anonymization to improve the fraud scoring engine	Legitimate interest in preventing payment fraud through OUR Services and complying with legal obligations (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 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 Maximum five (5) years for proven fraud

[1] As implemented by art. 47 of the Belgian Act of 11 March 2018 on the status and supervision of payment institutions and electronic money institutions, access to the business of payment service providers and to the activity of issuing electronic money, and access to payment systems

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
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 App	Legitimate interest to provide YOU with support, to answer questions or requests and to communicate changes to YOU (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
Responding to YOUR data subject request under the GDPR	Legal obligation under Chapter 3 of the GDPR (Art. 6.1.c of GDPR)	Any data needed to manage the request	Five (5) years from the response to the 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)	Legal obligation under Article 101 of the Payment Services Directive 2 (PSD2) (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	Legitimate interest in order to defend OUR rights (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/foreclosure period
Management and arbitration of commercial dispute resolution on the Wero dispute resolution platform	Performance of a contract (Art. 6(1)(b) GDPR)	Data related to the transaction (amount, timestamp) Data related to the Acceptor Shipping and billing address* Information about the dispute (reason for the dispute, message from the consumer)	Maximum five (5) years from the dispute resolution.
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 (as defined in the Wero General Terms & Conditions): external Id, name, date of birth, place of birth, location of residence. For USERS in an Open Banking Eligible Jurisdiction who intend to initiate Wero Transactions	Period of retention in accordance with legal and regulatory obligations (10 years for Anti-Money Laundering from the end of the contractual relationship and, in the case of data relating to Wero Transactions, ten years from their execution)

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
		from an Account with an Open Banking ASPSP, the information will be provided directly by the USER. WE may collect additional data directly from YOU where required by law such as the origin of your funds. Information concerning YOUR transactions performed through the Wero App.	
Measuring the performance of marketing actions	Consent (Article 6.1.a GDPR)	Information about YOU (Device identifiers, IP addresses). Information about YOUR use of OUR Services (analytics on how USERS interact with the app, battery status, internet connection, network connection, app's current view, date and time of the request, page title, page URL, referrer URL, screen resolution used, time in local USER's time zone, files that were clicked and downloaded, links to an outside domain that were clicked, page generation time, accept-language header, USER-Agent header). Diagnostic and performance information and crash data (e.g., technical logs related to app malfunctions).	1 year from the collection or when consent is withdrawn if earlier
Gathering insights on the use of the Services, improving and optimising the performance of OUR services (including the Wero App)	Where legally required, consent: i.e for the processing through non-essential cookies and tracking technologies (Article 6.1.a GDPR) In other cases, this processing is necessary for	Information about YOU (Device identifiers, IP addresses). Information about YOUR use of OUR Services (analytics on how USERS interact with the app, battery status, internet	1 year from the collection or when consent is withdrawn (where processing is based on consent) if earlier

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
	OUR legitimate interest in carrying out activities for the reporting on and improvement of the Services (Art. 6.1.f of GDPR)	connection, network connection, app's current view, date and time of the request, page title, page URL, referrer URL, screen resolution used, time in local USER's time zone, files that were clicked and downloaded, links to an outside domain that were clicked, page generation time, accept-language header, USER-Agent header). Diagnostic and performance information and crash data (e.g., technical logs related to app malfunctions).	
Crash reporting, analytics and fraud detection and security monitoring of the Wero App	Where legally required, consent: i.e. for the processing through non-essential cookies and tracking technologies (Article 6.1.a GDPR) In other cases, this processing is necessary for OUR legitimate interest in ensuring the stability and security, and improvement of the Services (Art. 6.1.f of GDPR)	Information about YOU (Device identifiers, IP addresses). Analytics on how USERS interact with the app, 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. Diagnostic and performance information and crash data (e.g., technical logs related to app malfunctions).	1 year from the collection or when consent is withdrawn (where processing is based on consent) if earlier

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
In the context of a corporate transaction – To evaluate or carry out an acquisition, merger, demerger, restructuring, reorganisation, dissolution or other sale or transfer of some or all of OUR assets, whether by way of transfer of all or part of the business, or as part of a bankruptcy, liquidation or similar proceeding, where Personal Data held by US forms part of the transferred assets	Legitimate interest in carrying out the said business transactions to implement OUR business strategies or grow OUR business (Art. 6.1.f of GDPR)	Any necessary data for the purposes of the corporate transaction.	Duration necessary to complete the corporate transaction.

*Depending on the bank of the Acceptor.

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 Device Biometric ID (such as YOUR fingerprint or face scan), to authenticate YOUR payments in the Wero App.

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.

Furthermore, for USERS who are Deutsche Bank customers, and only for these USERS, EPI acts as a Controller for the Processing of Personal Data described in Appendix 1 of this Policy.

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 conclusion and/or performance of OUR contract with YOU (as governed by the Wero General Terms & Conditions). 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 Datab are collected directly by EPI refer to section 3 and other provided to EPI by your ASPSPs.

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 ASPSP (as defined in the Wero General Terms & Conditions) 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 What are YOUR rights and how to exercise them?

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 or for the performance of a task carried out in the public interest, 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 Cookies and trackers Notice

The Wero App does not use traditional browser cookies, but it does rely on tracking technologies such as Software Development Kits (SDKs) and similar tools implemented in the mobile environment. These technologies enable the storage of or access to information on YOUR device for purposes such as crash diagnostics, user experience analytics, or marketing attribution.

All Processing of Personal Data collected via tracking technologies is covered by the other sections of this Privacy Policy.

The table below provides an overview of the tracking tools used in the Wero App, their purposes, the applicable legal basis under the ePrivacy Directive and the local implementations thereof such as the Belgian law of 30 July 2018, and the controls available to YOU as a USER.

- Essential cookies are strictly necessary for the proper functioning of the Wero App. These cookies do not require YOUR consent and cannot be disabled through the cookie banner or preference centre. Essential cookies are a no opt-out option however you have the right to object to the Personal Data as covered under section 7.

- Non-essential cookies are any cookies that are not strictly necessary for the Wero App to function. These cookies require the YOUR prior and explicit consent before being placed or read on the device. For Non-essential cookies, YOU have the option to remove YOUR consent.

<u>The consequences of accepting/refusing cookies:</u>

- YOU are free to accept or refuse Non-essential cookies at any time.
  Refusing cookies used for analytics and advertising purposes will not affect YOUR ability to access or navigate the Wero App. However, YOUR user experience may be less personalized, and WE may not be able to measure or improve the performance of our services as effectively.

- Accepting analytics cookies allows us to better understand how YOU interact with the Wero App and to optimize its design and functionality. Accepting advertising cookies enables us to provide YOU with more relevant ads and measure the effectiveness of our campaigns.

- YOUR choices will not affect essential cookies, which are strictly necessary for the Wero App to function properly.

Tool / Provider	Purpose	Period of retention	Legal Basis	User Controls
Instabug (Instabug Inc.)	Crash reporting – helps monitor bugs and ensure app stability.	Maximum 13 months as of collection	Exempt from consent: necessary to provide a stable app.	USERS may **opt out** via the app settings.
Matomo (InnoCraft Ltd)	UX analytics – helps improve navigation and interface design.	Maximum 13 months as of collection	Exempt from consent: necessary to optimize USER-requested service.	USERS may **opt out** via the app settings.
Adjust (Adjust GmbH)	Marketing attribution – measures performance of ad campaigns.	Maximum 13 months as of collection	Consent collected: • On **Android**, during onboarding (refusal disables tracking entirely)	USERS may **withdraw consent** at any time via the **app settings**

Tool / Provider	Purpose	Period of retention	Legal Basis	User Controls
			• On **iOS**, via App Tracking Transparency prompt. If declined, anonymous tracking is used via **SKAdNetwork**	(Android) or **device settings** (iOS).

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 Regulations, YOUR continued use of OUR Services following the posting of changes constitutes YOUR acceptance of such changes.

10.0 Contact

10.1 EPI

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

Address: de Lignestraat 13, 1000 Brussel, Belgium

Email: dpo@epicompany.eu

10.2 Data Protection Officer

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

Email: dpo@epicompany.eu

Last updated: 27/10/2025.

Appendix 1 - Processing activities only concerning USERS who are Deutsche Bank customers

This Appendix describes the specific Processing activities carried out by EPI in its capacity as Controller, which apply exclusively to USERS who are Deutsche Bank customers.

Purpose	Legal basis	Categories of Personal Data Processed	Retention period
Commercial transactions (Remote E/M-commerce transaction and point of sale Wero Transaction) orchestration	Performance of a contract (Art. 6(1)(b) GDPR)	Consent and transaction data; beneficiary data; technical identifiers related to the consumer and wallet data; refund data (where applicable).	Thirteen (13) months after the execution of the transaction.
Fraud prevention and fraud scoring during enrolment and provisioning of the Wero App	Legitimate interest in preventing payment fraud through OUR Services and ensuring the security of payment transactions (Art. 6.1.f GDPR)	Identification data (name, date of birth); payment account and wallet data; device and technical data; transaction data; fraud score and analytics data	Twenty-four (24) months from collection; up to five (5) years for confirmed fraud cases.
Strong Customer Authentication (SCA) for the initiation of a Wero Transaction, the validation of the consent and for the access to Account information	Legal obligation under Art. 97(1) PSD2 and corresponding national implementation (Art. 6.1.c GDPR)	Authentication token; technical identifiers; information about payment means; payment account and wallet data; transaction data	Thirteen (13) months after the execution of the transaction.
Chargeback management and dispute handling related to Wero Transactions	Performance of a contract (Art. 6(1)(b) GDPR)	Identification and contact data; transaction and consent data; dispute data	Five (5) years from the closure of the dispute or chargeback request.
Provision and operation of the Wero back-office platform	Legitimate interest in ensuring operational support and traceability of transactions (Art. 6.1.f GDPR)	Consumer and wallet data; transaction data; consent data	Duration of the contract with Deutsche Bank as EPI Member plus one (1) year for audit purposes.