

Privacy Policy for Users of MY WALL3T

Last updated: 10 September 2026

This Privacy Policy informs users of the MY WALL3T Wallet about the processing of personal data when using MY WALL3T.

MY WALL3T is designed so that, as a rule, the wallet can be used without providing a name or email address. Nevertheless, technical use may generate data that is classified as personal or pseudonymous data under data protection law.

The separate “Privacy Notice for Providers and Administrators of MY WALL3T” applies to contact persons, administrators and other authorised persons of providers.

1. Overview and controller

1.1 Controller

The controller responsible for the processing described in this Privacy Policy is:

W3B Solutions GmbH

Hardtstraße 16

59872 Meschede

Germany

Email: support@wb-solutions.org

Telephone: +49 291 9081113

hereinafter “MY WALL3T”, “we” or “us”.

1.2 Use without a personal user account

A personal user account with a name or email address is not required for ordinary use of the MY WALL3T Wallet.

For normal wallet use, users are, as a rule, not required to provide:

- names,
- email addresses,
- telephone numbers, or
- postal addresses.

1.3 Technical and pseudonymous data

MY WALL3T uses technical or pseudonymous identifiers so that digital content can be technically assigned to a wallet and managed within it.

Even if MY WALL3T does not know a user's name or email address, such technical identifiers may constitute personal or pseudonymous data under data protection law.

1.4 No individual wallet ID for providers

Providers do not receive an individual wallet ID that would allow them to recognise a user or wallet across multiple transactions.

Providers also do not receive wallet users' names, email addresses, telephone numbers or postal addresses via MY WALL3T.

2. Data when using MY WALL3T

2.1 Wallet and digital content

The following data in particular may be processed when using the wallet:

- technical wallet identifier,
- technical identifiers of digital content,
- type of digital content,
- issue or assignment of content,
- validity information,
- status of content,
- redemption,
- transfer,
- points entries,
- check-ins,
- technical time information, and
- further technical information required for the respective function.

Digital content may include, in particular:

- offers,
- vouchers,
- coupons,
- tickets,
- bonus points,
- permitted memberships, and
- other digital content supported by MY WALL3T.

Processing takes place in particular to provide the wallet, manage digital content, carry out redemptions and transfers, manage points and prevent misuse.

The legal basis is in particular Art. 6(1)(b) GDPR. Where processing serves security, misuse prevention or system stability, it may also be based on Art. 6(1)(f) GDPR.

2.2 Vouchers, tickets and redemptions

When digital content is redeemed, MY WALL3T processes the information required to technically check its validity and status and record the redemption.

This may include, in particular:

- technical wallet assignment,
- digital content identifier,
- provider or offer assignment,
- time of redemption, and
- redemption status.

The provider does not receive an individual wallet ID that would allow the wallet to be recognised across multiple transactions.

Where goods or services are purchased in connection with an offer, voucher, coupon or ticket, the respective provider, as a rule, supplies the goods or services directly.

MY WALL3T does not process any payment between user and provider for this purpose.

2.3 Bonus points

Where users can receive, use or transfer bonus points, MY WALL3T processes the technical transaction information required for this purpose.

This may include, in particular:

- number of points,
- time of the entry,
- type of entry,
- technical wallet assignment, and
- assignment to the relevant points programme.

2.4 Check-ins

Where a user uses a check-in function, the following in particular may be processed:

- technical wallet assignment,
- check-in or provider/campaign assignment,
- time of the check-in, and
- information for implementing repeat-use restrictions.

Check-in data is, as a rule, stored for up to 24 months.

2.5 Permitted memberships

MY WALL3T does not permit memberships or comparable digital content that may reveal special categories of personal data within the meaning of Art. 9(1) GDPR.

In particular, memberships from which inferences can be drawn about the following are prohibited:

- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health data,
- genetic data,
- biometric data for identification purposes,
- sex life, or
- sexual orientation.

MY WALL3T is therefore not designed to process special categories of personal data through memberships.

2.6 Transfer of the wallet

MY WALL3T provides a function for transferring or restoring the wallet on another device.

A private key or a corresponding transfer credential is used for this purpose.

The private key serves to authorise the intended wallet transfer function.

Users are responsible for keeping the private key safe and protecting it against access by unauthorised third parties.

Without the required private key, the transfer function provided for this purpose cannot be used.

3. Device data, location and push notifications

3.1 Location functions

Certain functions of MY WALL3T may use the device's current location.

Location processing takes place only if the user expressly uses a corresponding function and has granted the required device permission.

Depending on the function, current location information may be processed.

MY WALL3T does not use location information to create movement profiles or for personalised advertising.

No general permanent location history is created.

Location permissions can be changed or withdrawn through the operating system settings.

Location-dependent functions may subsequently be restricted.

3.2 Push notifications

Push notifications are used only if the user has activated this function or granted the required permission.

The Apple Push Notification Service (APNs) may be used on Apple devices.

The following in particular may be processed:

- push or device token, and
- content of the message to be transmitted.

Firebase Cloud Messaging (FCM) may be used on Android devices.

The following in particular may be processed:

- push token,
- pseudonymous installation identifier,
- IP address, and
- content of the message.

MY WALL3T does not use Firebase Analytics.

As a rule, push tokens are stored for as long as push notifications are activated, the wallet exists and the token is technically valid.

3.3 App stores

When users download or update MY WALL3T through an app store, the respective app store operator processes data under its own responsibility.

MY WALL3T may be provided in particular through:

- Apple App Store,
- TestFlight, and
- Google Play.

The respective store operators may process, in particular, app store account data, device information and download, update and diagnostic data.

4. Technical infrastructure and external services

4.1 Hosting

The server side of MY WALL3T is operated using Google Cloud services.

Under the current technical configuration, the server components, including databases and uploads, are operated in the region:

europe-west3 - Frankfurt am Main, Germany

The technical infrastructure serves in particular to provide the wallet, manage digital content, process transactions and ensure the security and stability of the platform.

4.2 Server and security logs

Technically necessary server and security logs may be created when MY WALL3T is accessed.

The following in particular may be processed:

- IP address,
- time of access,
- resource accessed,
- technical request information,
- device or client information, and
- security-relevant events.

Processing serves in particular secure and stable operation, detection and prevention of attacks and error analysis.

The legal basis is Art. 6(1)(f) GDPR.

Server and security logs are, as a rule, stored for up to 30 days.

4.3 Error analysis with Sentry

We use Sentry for technical error detection and to stabilise MY WALL3T.

Under the current technical configuration, the provider is Functional Software, Inc., USA.

The following in particular may be processed:

- IP address,
- device type,
- operating system,
- app version,
- time of an error, and
- technical error details.

Additional personal content data is not intended to be deliberately transmitted to Sentry in the production environment.

Sentry error data is, as a rule, stored for up to 90 days.

The legal basis is Art. 6(1)(f) GDPR.

4.4 Data backup and backups

We create technical backup copies to ensure the availability, integrity and recoverability of our systems.

Under the current technical configuration, in particular:

- daily database backups, and
- continuous backups of changes for point-in-time recovery

are used.

The backups are stored in the EU region europe-west3 - Frankfurt am Main.

The backup copies are stored and transmitted in encrypted form.

Backups serve exclusively:

- data backup,
- IT security,
- recovery, and
- emergency preparedness.

They are not used for marketing or analysis purposes.

Deleted or anonymised data may still be temporarily contained in existing backup copies.

These backup copies are automatically deleted after no more than 30 days.

4.5 Mapbox

MY WALL3T may use Mapbox for map displays and location-related functions.

When corresponding functions are used, the following in particular may be processed:

- IP address,
- device or browser information,
- map area, and
- where applicable, the current location, to the extent technically necessary for the function activated by the user.

4.6 Google Maps

Google Maps may be used on certain public offer pages.

Google Maps is not loaded automatically there merely by opening the page.

Data may be transferred to Google only when the user activates a corresponding function such as “Load map”.

4.7 YouTube

Where MY WALL3T provides embedded YouTube content, it is not automatically activated when the relevant page is opened.

Under the intended technical design, embedding takes place via youtube-nocookie.com and requires prior activation.

Data may be transferred to YouTube or Google only when the user actively loads or plays the content.

4.8 Fonts

Under the current technical configuration, fonts used by MY WALL3T are provided locally or through its own infrastructure.

Merely displaying these fonts therefore does not establish a connection to Google Fonts.

5. Other services, providers and user groups

5.1 Relationship with providers

Providers do not receive personal master data of wallet users via MY WALL3T.

In particular, they do not receive:

- names,
- email addresses,
- telephone numbers,
- postal addresses, or
- individual wallet IDs

that would allow a wallet to be recognised across multiple transactions.

Where providers receive statistical information, it is provided in anonymous or aggregated form.

5.2 No processing on behalf of providers

Under the current technical configuration, MY WALL3T does not process personal data of wallet users on behalf of providers.

As a rule, therefore, there is no controller-processor relationship under Art. 28 GDPR between W3B Solutions GmbH and providers with regard to the ordinary processing of wallet user data.

5.3 Data outside MY WALL3T

If a user provides personal data to a provider outside MY WALL3T, for example in connection with a purchase or another business relationship, the respective provider is, as a rule, itself responsible for this under data protection law.

5.4 No payment data

MY WALL3T does not process users' payments for a provider's goods or services.

In connection with these transactions, MY WALL3T therefore does not process, in particular, credit card, bank account or other payment data of the wallet user.

5.5 No general advertising or user analysis

Under the current technical configuration, MY WALL3T does not use general analysis or tracking systems to create user profiles for personalised advertising.

In particular, the following are not currently used:

- advertising IDs for personalised advertising,
- Firebase Analytics profiles, or
- session replay systems to observe wallet use.

Technically necessary security, error and functional data remain unaffected.

6. Recipients and international data transfers

6.1 Recipients

Personal data is disclosed only to the extent required for the purposes described or where a statutory obligation exists.

Recipients may include, in particular:

- hosting and infrastructure providers,
- IT and security service providers,
- error analysis and monitoring service providers,
- push services,
- map and geodata services,
- providers of embedded external content, and
- authorities or courts where a corresponding statutory obligation exists.

6.2 Third countries

Some service providers used are based in the USA or may have another connection to a third country.

Personal data is transferred to countries outside the European Economic Area only in compliance with the conditions of Art. 44 et seq. GDPR.

Depending on the recipient, the transfer may be based in particular on:

- an adequacy decision of the European Commission,
- an applicable recognised adequacy mechanism,
- standard contractual clauses of the European Commission, or
- another legally permissible transfer mechanism.

Where required, we take additional safeguards into account.

7. Retention period, deletion and anonymisation

7.1 General principle

As a rule, we store personal data only for as long as required for the respective purpose.

7.2 Wallet data

As a rule, the data required for the wallet is processed for as long as the wallet exists.

7.3 Transactions and entries

As a rule, information about the award, redemption, transfer and other technically necessary entries relating to digital content is assigned to the wallet for as long as the wallet exists.

There is currently no uniform fixed deletion period for these transactions.

When the wallet is deleted or anonymised, the wallet assignment is removed or replaced with a neutral placeholder in accordance with the technical deletion concept.

Where transaction information is subsequently required exclusively for non-personal statistical purposes, it may continue to be maintained without a personal wallet reference.

7.4 Check-ins

As a rule, check-in data is stored for 24 months.

7.5 Redemption and membership codes

Depending on their function, technical redemption or membership codes may be stored without a direct user reference.

There is currently no uniform fixed retention period for such codes where they are required for the technical functioning of the respective content.

7.6 Expired and redeemed vouchers or tickets

Expired, invalid or redeemed digital content may continue to be stored within the wallet as evidence or to display previous wallet content.

As a rule, it is deleted together with the wallet or separated from the wallet assignment upon anonymisation.

7.7 Ended memberships

Data on ended permitted memberships is, as a rule, stored for up to 24 months where required for technical documentation.

7.8 Inactive wallets

If a wallet is not used for a period of 36 months, it may be anonymised in accordance with the Terms of Use.

Upon anonymisation, the personal or pseudonymous assignment of the wallet is removed in accordance with the technical deletion concept.

Any remaining points and outstanding vouchers or tickets may thereby expire or become unusable in accordance with the Terms of Use.

Where push notifications are activated and technically deliverable, the user may be informed approximately three months before the planned anonymisation.

7.9 Deletion of the wallet

Users can delete their wallet in accordance with the functions provided in MY WALL3T.

Upon deletion, the personal or pseudonymous data assigned to the wallet is deleted or anonymised in accordance with the technical deletion concept, unless compelling statutory or technical reasons require temporary further processing.

Existing backup copies are not subsequently modified individually.

Data contained in them is deleted no later than the end of the 30-day backup cycle.

7.10 Further retention periods

Data type	Regular retention period
Server and security logs	up to 30 days
Sentry error data	up to 90 days
Check-in data	up to 24 months
Ended permitted memberships	up to 24 months
Inactivity until anonymisation	36 months
Backups	no more than 30 days
Location data	only for as long as required for the activated function
Push tokens	until deactivation, wallet deletion/anonymisation or invalidity

8. Legal bases and users' rights

8.1 Legal bases

We process personal data in particular on the following legal bases:

Art. 6(1)(a) GDPR

where consent is required for specific processing.

Art. 6(1)(b) GDPR

where processing is necessary to provide MY WALL3T and the functions requested by the user.

Art. 6(1)(c) GDPR

where processing is necessary for compliance with a legal obligation.

Art. 6(1)(f) GDPR

where processing is necessary for the purposes of our legitimate interests or those of a third party and is not overridden by the interests or fundamental rights and freedoms of the user.

Our legitimate interests include, in particular:

- secure operation of MY WALL3T,
- IT security,
- misuse prevention,
- error analysis,
- ensuring system stability,
- data backup and recovery, and
- establishing, exercising or defending legal claims.

8.2 Device permissions

Device permissions, for example for location or push notifications, can be managed and withdrawn through the settings of the respective operating system.

Where processing is based on consent under data protection law, that consent may be withdrawn at any time with effect for the future.

8.3 Obligation to provide data

For ordinary use of MY WALL3T, users are, as a rule, not required to provide a name or email address.

However, certain technical data is required to provide the wallet and the functions requested in each case.

If technically necessary data is not processed or required device permissions are not granted, individual functions may be unavailable or usable only to a limited extent.

8.4 Automated decisions

As a rule, the processing described does not involve a decision based solely on automated processing that produces legal or similarly significant effects within the meaning of Art. 22 GDPR.

Technical checks, for example of the validity or prior redemption of digital content, remain unaffected.

8.5 Data subject rights

Subject to the statutory conditions, users have in particular the right to:

- access under Art. 15 GDPR,
- rectification under Art. 16 GDPR,
- erasure under Art. 17 GDPR,
- restriction of processing under Art. 18 GDPR,
- data portability under Art. 20 GDPR, and
- object under Art. 21 GDPR.

Since MY WALL3T can, as a rule, be used without a name or email address, handling a data subject right may require the user to establish an appropriate technical link to the wallet or transaction concerned.

Only additional information required for this assignment will be requested.

8.6 Objection under Art. 21 GDPR

Where we process personal data on the basis of Art. 6(1)(f) GDPR, the user has the right to object to that processing at any time on grounds relating to their particular situation.

We will then no longer process the personal data concerned unless we can demonstrate compelling legitimate grounds for the processing that override the user's interests, rights and freedoms, or the processing serves to establish, exercise or defend legal claims.

8.7 Right to lodge a complaint

Users have the right to lodge a complaint with a data protection supervisory authority if they consider that the processing of their personal data infringes the GDPR.

8.8 Contact for data protection enquiries

For questions about data protection or to exercise data subject rights:

W3B Solutions GmbH

Hardtstraße 16

59872 Meschede

Germany

Email: support@wb-solutions.org

8.9 Changes to this Privacy Policy

We may amend this Privacy Policy if changes occur in particular to:

- functions of MY WALL3T,
- technical processes,
- service providers used,
- data processing, or
- legal requirements.

The current version made available at the relevant time is authoritative.

Distinction regarding providers

This Privacy Policy concerns use of the MY WALL3T Wallet by users.

For personal data of:

- providers,
- providers' contact persons,
- administrators, and
- other authorised persons of a provider,

the following separate notice applies:

“Privacy Notice for Providers and Administrators of MY WALL3T”

W3B Solutions GmbH

Hardtstraße 16

59872 Meschede

Germany

Email: support@wb-solutions.org

MY WALL3T - Privacy Policy for Users

Last updated: 10 September 2026