

Privacy Policy for Users of MY WALL3T

Last updated: 29 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 the Wallet can generally be used **without providing a name or email address**. Nevertheless, technical use may generate data that qualifies 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@mywall3t.net

Telephone: +49 291 9081113

hereinafter referred to as "**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 generally do not have 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 the Wallet.

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 Providers Do Not See a Cross-Provider Individual Wallet ID

Providers receive **no cross-provider Wallet ID** - providers see only a provider-specific pseudonymous identifier. This allows them to recognise a Wallet in their own transactions, but they cannot link it to transactions with other providers.

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

2. Data when Using MY WALL3T

2.1 Wallet and Digital Content

When the Wallet is used, the following data in particular may be processed:

- technical Wallet identifier,
- technical identifiers of digital content,
- type of digital content,
- issuance or assignment of content,
- validity information,
- status of content,
- redemption,
- transfer of transferable digital content,
- points entries and exchange of bonus points for vouchers, tickets and offers,
- check-ins,
- technical timestamps 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 is carried out in particular to provide the Wallet, manage digital content, carry out redemptions and transfers of transferable digital content, manage points and their exchange for vouchers, tickets and offers, and prevent abuse. The legal basis is, in particular, Article 6(1)(b) GDPR. Where processing serves the security, abuse prevention or stability of the systems, it may also be based on Article 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,
- identifier of the digital content,
- assignment to a provider or offer,
- time of redemption and
- redemption status.

The provider does not receive a cross-provider Wallet ID - providers see only a provider-specific pseudonymous identifier. This allows them to recognise a Wallet in their own transactions, but they cannot link it to transactions with other providers. Where goods or services are purchased in connection with an offer, voucher, coupon or ticket, the respective provider generally supplies them directly.

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

2.3 Bonus Points

Where users receive bonus points and exchange them in the MY WALL3T marketplace for vouchers, offers or tickets from providers participating in the respective points programme, MY WALL3T processes the technical booking information required for this purpose. This may include, in particular:

- number of points,
- time and type of entry,
- technical Wallet assignment,
- assignment to the relevant points programme,
- assignment of the exchange to the participating provider and the offer or ticket obtained in the exchange, and
- status of the exchange.

Bonus points are not transferred between users. The transfer of other digital content remains unaffected.

2.4 Check-ins

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

- technical Wallet assignment,
- assignment to a check-in or provider/promotion,
- time of the check-in and
- information for implementing restrictions on repeated check-ins.

Check-in data is generally 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 Article 9(1) GDPR. In particular, memberships that allow inferences to be drawn about the following are not permitted:

- 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. For this purpose, 24 recovery words or an equivalent transfer credential are used. The recovery words serve to authorise the designated Wallet transfer function. Users are responsible for storing the recovery words securely and protecting them against access by unauthorised third parties. Without the recovery words, the transfer function provided for this purpose cannot be used.

3. Device Data, Location and Push Notifications

3.1 Location Functions

Certain MY WALL3T functions may use the device's current location. Location data is processed only if the user expressly uses a corresponding function and has granted the necessary 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 continuous location history is created. Location permissions can be changed or withdrawn via the operating system settings. Location-dependent functions may subsequently be limited.

3.2 Push Notifications

Push notifications are used only if the user has activated this function or granted the necessary permission. On Apple devices, the Apple Push Notification Service (APNs) may be used. The following in particular may be processed:

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

On Android devices, Firebase Cloud Messaging (FCM) may be used. The following in particular may be processed:

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

MY WALL3T does not use Firebase Analytics. Push tokens are generally 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 made available 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

MY WALL3T is operated on the server side 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 to ensure secure and stable operation, detect and defend against attacks, and analyse errors. The legal basis is Article 6(1)(f) GDPR. Server and security logs are generally stored for up to 30 days.

4.3 Error Analysis with Sentry

We use Sentry to detect technical errors and 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 generally stored for up to 90 days. The legal basis is Article 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 design, the following in particular are used:

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

The backups are stored in the EU region europe-west3 - Frankfurt am Main. Backup copies are stored and transmitted in encrypted form. Backups serve exclusively for:

- data backup,
- IT security,
- recovery and
- contingency planning.

They are not used for marketing or analysis purposes. Deleted or anonymised data may temporarily remain in existing backup copies. These backup copies are automatically deleted after 30 days at the latest.

4.5 Mapbox

MY WALL3T may use Mapbox for map displays and location-based functions in the web marketplace - and therefore in the marketplace view of the app. When corresponding functions are used, the following in particular may be processed:

- IP address,
- device or browser information,

- map area displayed and
- where applicable, the current location, insofar as this is technically necessary for the function activated by the user.

4.6 Google Maps

A link to Google Maps may be used on certain public offer pages. Google Maps is not loaded automatically merely by accessing those pages. Data may be transmitted to Google only when the user activates the link.

4.7 YouTube

Where MY WALL3T provides embedded YouTube content, this is not activated automatically when the relevant page is accessed. Under the intended technical design, content is embedded via youtube-nocookie.com and requires prior activation. Data may be transmitted to YouTube or Google only when the user actively loads or plays the content.

4.8 Fonts

Under the current technical design, 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 through MY WALL3T. In particular, they do not receive:

- names,
- email addresses,
- telephone numbers,
- postal addresses or
- cross-provider Wallet IDs (providers see only a provider-specific pseudonymous identifier. This allows them to recognise a Wallet in their own transactions, but they cannot link it to transactions with other providers)

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

5.2 No Processing on Behalf of Providers

Under the current technical design, MY WALL3T does not process Wallet users' personal data on behalf of providers. Consequently, there is generally no controller-processor relationship under Article 28 GDPR between W3B Solutions GmbH and the 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 generally itself responsible for this under data protection law.

5.4 No Payment Data

MY WALL3T does not process users' payments for goods or services of a provider. In the context of these transactions, MY WALL3T therefore does not process, in particular, the Wallet user's credit card, bank account or other payment data.

5.5 No General Advertising or User Analytics

Under the current technical design, MY WALL3T does not use general analytics or tracking systems to create user profiles for personalised advertising. In particular, the following are currently not used:

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

Technically necessary security, error and functional data remains unaffected.

6. Recipients and International Data Transfers

6.1 Recipients

Personal data is disclosed only insofar as this is necessary for the purposes described or there is a legal obligation. 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 there is a corresponding legal obligation.

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 requirements of Articles 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 necessary, we take additional safeguards into account.

7. Retention Period, Erasure and Anonymisation

7.1 General Principle

We generally store personal data only for as long as necessary for the respective purpose.

7.2 Wallet Data

The data required for the Wallet is generally processed for as long as the Wallet exists.

7.3 Transactions and Booking Processes

Information on the award and exchange of bonus points for vouchers, offers or tickets, as well as the redemption and transfer of other transferable digital content and other technically necessary booking processes, is generally assigned to the Wallet for as long as the Wallet exists. There is currently no uniform fixed erasure period for these processes. When the Wallet is deleted or anonymised, the Wallet assignment is

removed or replaced with a neutral placeholder in accordance with the technical erasure concept. Where booking information is subsequently required exclusively for statistical purposes that do not involve personal data, it may be retained without a personal link to the Wallet.

7.4 Check-ins

Check-in data is generally stored for up to 24 months.

7.5 Redemption and Membership Codes

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

There is currently no uniform fixed retention period for such codes insofar as they are needed for the technical functionality 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. It is generally deleted together with the Wallet or, in the case of anonymisation, disconnected from its Wallet assignment.

7.7 Ended Memberships

Data on ended permitted memberships is generally stored for up to 24 months insofar as this is necessary 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. Anonymisation removes the personal or pseudonymous assignment of the Wallet in accordance with the technical erasure concept. Any remaining points and outstanding vouchers or tickets may 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 using the functions provided in MY WALL3T. Upon deletion, the personal or pseudonymous data assigned to the Wallet is erased or anonymised in accordance with the technical erasure concept, unless there are compelling legal or technical reasons for temporary continued processing. Existing backup copies are not subsequently modified individually. Data contained in them is erased no later than the end of the 30-day backup cycle.

7.10 Other Retention Periods

Data type - Usual 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 - maximum 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: Article 6(1)(a) GDPR where consent is required for a particular processing activity. Article 6(1)(b) GDPR where processing is necessary to provide MY WALL3T and the functions requested by the user. Article 6(1)(c) GDPR where processing is necessary for compliance with a legal obligation. Article 6(1)(f) GDPR where processing is necessary for the purposes of our legitimate interests or those of a third party and these are not overridden by the user's interests or fundamental rights and freedoms. Our legitimate interests include, in particular:

- secure operation of MY WALL3T,
- IT security,
- abuse prevention,
- error analysis,
- ensuring system stability,
- data backup and recovery, and
- establishment, exercise or defence of legal claims.

8.2 Device Permissions

Device permissions, for example for location or push notifications, can be managed and withdrawn via the settings of the respective operating system. Where processing is based on consent under data protection law, this 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 generally do not have to provide a name or email address. However, certain technical data is required so that the Wallet and the respective desired functions can be provided. If technically necessary data is not processed or required device permissions are not granted, individual functions may not be available or may be available only to a limited extent.

8.4 Automated Decisions

In the context of the processing described, there is generally no decision based solely on automated processing that produces legal or similarly significant effects within the meaning of Article 22 GDPR. Technical checks, for example regarding the validity or prior redemption of digital content, remain unaffected.

8.5 Data Subject Rights

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

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

As MY WALL3T can generally be used without a name or email address, handling a data subject rights request may require the user to establish an appropriate technical link to the relevant Wallet or

transaction. Only such additional information as is necessary to establish this link will be requested.

8.6 Objection under Article 21 GDPR

Where we process personal data on the basis of Article 6(1)(f) GDPR, the user has the right to object to this 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 which override the user's interests, rights and freedoms, or the processing serves the establishment, exercise or defence of 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@mywall3t.net

8.9 Changes to this Privacy Policy

We may amend this Privacy Policy if, in particular, any of the following change:

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

The current version made available at the relevant time applies.

Distinction from Providers This Privacy Policy concerns users' use of the MY WALL3T Wallet. Personal data of:

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

is covered by the separate: "Privacy Notice for Providers and Administrators of MY WALL3T".

W3B Solutions GmbH
Hardtstraße 16
59872 Meschede
Germany
Email: support@mywall3t.net

MY WALL3T - Privacy Policy for Users

Last updated: 29 September 2026