

Plenzo Privacy Policy

How we collect, process, protect and retain your data across Plenzo.

Version 3.3 · Effective from 18 October 2026 · Durable copy: [privacy-en-v3.3.pdf](#)

Current version: <https://www.plenzo.app/en/legal/privacy>

Document details

Effective from 18 October 2026. Version 3.3.

1. Data controller and contact

The controller of your personal data is PLENZO sp. z o.o., with its registered office in Warsaw, Aleje Jerozolimskie 47/34, 00-697 Warsaw, Poland.

For matters concerning the processing of personal data and the exercise of your rights, contact us at privacy@plenzo.app or in writing at our registered office. Security reports, including suspected unauthorised access to an account or a vulnerability in our systems, should be sent to security@plenzo.app.

2. Scope of this Policy

This Policy describes the processing of personal data in connection with the [plenzo.app](#) website, the Plenzo app for iOS and Android, and communication with Plenzo. It also covers people using test versions and early access to the app.

It applies to website visitors, app users, people subscribed to the newsletter, and people contacting us by email, the in-app form, social media and discussion services. It also covers interactions with Plenzo profiles and posts, such as comments and replies on Reddit.

The app, participation in testing, and signing up to the newsletter are intended for people aged 18 or over.

The scope of the data we process depends on the features you use. Operators of social media and discussion services also process data on their own terms, described in their privacy policies. Information about cookies and similar technologies on the website is set out in the [Cookies Policy](#).

If you use our profiles on Facebook or Instagram, Plenzo and Meta Platforms Ireland Limited are joint controllers of the statistical data concerning those profiles, processed under the joint-controller arrangements made available by Meta; Meta is responsible for fulfilling your rights in respect of those statistics. Other platforms, including TikTok, LinkedIn, YouTube and Reddit, process data about your interactions with our profiles as separate controllers, on the terms described in their privacy policies.

3. Your account and use of the app

We use Amazon Web Services (AWS) to handle registration and sign-in. You can sign in with an email address and password or with a Google account, and on iOS also with an Apple account.

We process your email address, account identifier, authentication data and information needed to maintain your session. Password handling is provided by the AWS authentication service. When you sign in with Apple or Google, we use your user identifier and email address.

In your profile we store the date the account was created, the interface language, the currency you selected, the time zone we use to determine the days of your transactions and the current month, your money-management settings and the status of your analytics consent. If you provide a first name in your profile settings, we also process that information.

When you create an account we also record which version of the Terms you accepted and when, and that you declared you are aged 18 or over. We do not collect your date of birth and we do not verify your age — we rely on your declaration. This record serves to demonstrate the terms on which the contract was concluded and that the conditions for concluding it were met. After the contract is concluded, we send a confirmation together with a copy of the accepted version of the Terms to your email address.

We process the data needed to create and operate your account, to make the money-management features you choose available to you, and to manage access to paid features, in order to perform the contract for the provision of Plenzo services — Article 6(1)(b) GDPR.

Providing the data required to create an account is a condition of using it. You provide or share other data depending on the features you choose; without the data necessary for a given feature, we cannot provide it.

4. Financial data and its analysis

If you choose to connect a bank account, Tink AB provides you with an account information service under a separate agreement whose terms are presented in Tink Link. There, you authorise Tink to access your account and share the data with Plenzo. Tink is a separate controller of the data processed when providing that service; its processing is described in the privacy notice available in Tink Link. Authorisation to access your account does not replace consent to the separate processing purposes described in this Policy.

We receive account data from Tink, including the account's name, type, currency and balance, together with your transaction history. Transaction data includes, among other things, amounts, dates, descriptions, the names of senders and recipients, and information used for categorisation. From the time this data is made available to Plenzo, we are its controller for processing for our services described in this Policy. Plenzo does not receive your bank login credentials and does not initiate payments through these connections.

We store transaction dates as your bank provides them: the booking date and time and — where your bank provides them — the date and time the transaction was made.

Account data may also include the name of the account holder, used to recognise transfers between your own accounts.

We also process financial data you enter in the app, including manually added transactions, budgets, goals, tags, asset information and notes.

To show you the time of a purchase as it was where you made it, and to assign each transaction to the right day, the app sends us the identifier of the time zone set on your device, for example Europe/Warsaw or Asia/Tokyo, and the moment it changed. We do not collect GPS location or addresses for this, but a time zone indicates approximately the country or region you are in. On this basis we store, with each transaction, the time zone of the place of purchase. You can also assign a time zone to a trip you create in

the app. The legal basis is the performance of the contract for the provision of Plenzo services — Article 6(1)(b) GDPR.

We analyse your financial data automatically in order to categorise transactions, recognise recurring payments, and present you with summaries, suggestions and notifications. Spending comparisons refer to your own history.

Plenzo does not use the results of these analyses to make decisions about access to the service or to set individual pricing. We do not make decisions about you based solely on automated processing that would produce legal effects concerning you or similarly significantly affect you.

Transaction data received from your bank through Tink may contain data about other people, including the names of the senders or recipients of transfers. We store this data together with the transactions and use it to recognise and present those transactions to the user and to identify transfers between the user's own accounts.

The basis for processing these people's data is the legitimate interest of Plenzo and of the user in enabling the transaction history to be viewed and organised — Article 6(1)(f) GDPR.

We use this data to show you your transaction history and to recognise transfers between your accounts. We do not create profiles of these people, we do not combine their data across users, and we do not use it for marketing or analytics. We store it for as long as the transaction it relates to, and delete it together with that transaction. We have no way of contacting these people directly, which is why we provide information about the processing in this Policy. If you are such a person and wish to object or request erasure, write to privacy@plenzo.app.

Transactions may also reveal information concerning health. Before the first synchronisation of an account, we ask whether we may store bank-provided details of transactions recognised as relating to healthcare and optical care, automatically assign the corresponding categories and use this information in your budgets, summaries and analyses. The basis for this processing is your explicit consent — Article 6(1)(a) and Article 9(2)(a) GDPR. Regardless of this decision, you can manually assign a transaction to "Health / doctor and healthcare" or "Optical care".

Consent is voluntary and you can withdraw it in settings. If you do not give consent, or you withdraw it, we do not store or use the transaction's bank-provided description, the recipient's name, an automatically assigned healthcare category or other information from the bank or automatic recognition that indicates the provider or type of service. We retain the data needed for your totals and balance to remain accurate: the amount, currency, date, account, booking status and technical transaction identifier. We also retain a category you manually assigned to a specific transaction; you can change or remove it yourself. After consent is withdrawn, we delete previously retained bank details, automatically assigned healthcare categories and data created solely from them within 30 days at the latest; this does not remove your manual category assignments. Renewed consent covers data received from the moment it is given; we do not restore details deleted earlier.

The Pharmacy, Beauty and Health and beauty — other categories are separate from the Health / doctor and healthcare and Optical care categories. Assigning a transaction to Pharmacy, Beauty or Health and beauty — other does not by itself mean that we treat it as data concerning health. You can manually assign, change and remove the Health / doctor and healthcare and Optical care categories regardless of your consent decision. Expenses assigned this way are included in budgets, budget coverage, Saver cuts

and limit notifications. Without consent, we do not automatically assign these categories to subsequent transactions.

Transactions recognised as a payment to a church, parish or other religious organisation, a political party, or a trade union may indirectly reveal your religious beliefs, political opinions or trade union membership. We record such transactions only with the data needed for settlement: the amount, currency, date, account, booking status and technical transaction identifier, without the description from your bank, the recipient's name or a category. We do not ask for consent to this processing, because this data is never stored in the first place.

5. Purchases and subscriptions

Plenzo subscriptions are purchased solely through the App Store or Google Play. Payments are handled by Apple or Google respectively, under their own privacy terms. Plenzo processes information about the purchase and the subscription status in order to manage access to paid features, on the basis of performance of the contract — Article 6(1)(b) GDPR.

We delete information about purchases and subscription status together with your account. If, during the paid period, you create a new account on a device signed in to the same App Store or Google Play account, the store will confirm the purchase to us and we will restore access until the end of that period. Deleting your account does not cancel the subscription in the App Store or Google Play — you manage cancellation in that store.

6. Contact, support and feature suggestions

When you contact us, we process your contact details or username, the content of the correspondence and any attachments you add voluntarily. In the in-app form we also process the type of request, the app version and platform, and information enabling us to link the request to your account and establish when we received it.

We use this data to respond, handle requests and complaints, diagnose errors, and analyse feedback and suggestions for developing Plenzo.

Where the contact concerns help necessary to perform the contract for the use of Plenzo, the basis for processing is Article 6(1)(b) GDPR. For other questions and suggestions, the basis is our legitimate interest in conducting correspondence and handling requests — Article 6(1)(f) GDPR.

Please share only the information needed to handle the matter. Before adding an attachment, remove or redact unnecessary personal and financial data, especially data concerning other people. Do not send passwords or banking access codes.

7. Email communication and newsletter

We process your email address and the information needed to handle correspondence, newsletter sign-up, and the documentation of consent given and withdrawn. When you subscribe to the newsletter, we also record the accepted version and language of the Newsletter Terms, the date of acceptance, and your declaration that you are aged 18 or over.

We send messages needed to operate your account and the service, including the confirmation of the account agreement, and messages about security, your requests, participation in testing, and changes

affecting your use of Plenzo. These do not require a newsletter sign-up; we rely on the basis appropriate to the matter concerned, as described in this Policy.

To demonstrate that we provided information about changes to legal documents, we keep the email address, language and source of the address (a Plenzo account or newsletter), the document's name and version, the content of the notice, and information about sending, acceptance by the email provider, delivery, failures and retries. This evidence demonstrates that information was provided and supports the establishment, exercise or defence of legal claims. The legal basis is our legitimate interest (Article 6(1)(f) GDPR). We do not collect information about opens or clicks for this purpose.

We process data for sending the newsletter and marketing messages on the basis of your consent — Article 6(1)(a) GDPR. Messages are sent within the scope of the consent you gave for email communication. They may include information about the availability and features of the App, updates, offers and promotions of Plenzo, and educational content about personal finance. Creating an account or taking part in testing does not in itself constitute consent to marketing. Unsubscribing from the newsletter does not limit your use of the App. The rules for providing the newsletter are set out in the Newsletter Terms.

You can opt out of marketing communication at any time using the link in a message or by writing to privacy@plenzo.app. After you opt out, we may still send messages needed to operate your account, handle your requests or comply with legal obligations.

After you unsubscribe, we mark the subscription as inactive. We retain your email address and the record of your opt-out in order to respect your choice. We also retain documentation of consent and its withdrawal, covering the dates, the manner and the source of those actions, and the version of the consent wording. This documentation does not entitle us to send further marketing on the basis of withdrawn consent. Deleting your account does not automatically delete this documentation.

We use Resend to send messages and to receive replies to support messages. In connection with this handling, Resend processes sender and recipient addresses, the subject and content of the message, and information about the message being sent, received and delivered.

8. App and website analytics

With your consent, we analyse how you use the app and the plenzo.app website in order to assess the use of features and improve them. We use PostHog for this purpose. The legal basis for the processing is consent — Article 6(1)(a) GDPR.

For app and website analytics we use PostHog EU Cloud. Analytics data is stored on servers in Frankfurt, Germany, within the European Economic Area. Information about processing outside the EEA and the safeguards applied is set out in section 12.

Consent to website analytics and consent to app analytics are separate. Giving or withdrawing one does not change the other. We ask for consent to website analytics in a banner on your first visit, and you can change your choice at any time through the cookie settings in the website footer. Details of cookies and browser storage are set out in the Cookies Policy.

We ask for consent to app analytics during onboarding and in the app settings. Consent is voluntary. You can refuse it or withdraw it at any time in the app settings; that decision does not affect access to features

or to the entitlements under your plan. When consent is withdrawn, we stop further analytics of your use of the app.

Your new app analytics choice — whether you give or refuse consent — applies to your account and all devices on which you are signed in. Reinstalling the app or changing your phone does not require you to make that choice again. Withdrawing consent on one device also stops account analytics on your other devices.

Previously recorded choices with a specified end date or limited to a particular installation keep those limits. We do not extend them in time or to other devices automatically; the new scope requires your new, active choice.

App analytics covers screen views and selected actions, such as opening or completing a feature, and limited technical information about errors and execution time. With your consent, we also measure use of the Plenzo Plus offer: viewing the offer, selecting a plan and the outcome of a purchase attempt. Events include the app version and platform, operating system version, general device type and interface language. We do not send bank transaction amounts or descriptions, merchant or payee names, balances, assessments of your financial situation, time zones, or financial record and payment identifiers to this analytics. We do not record sessions or content entered on screens. Consent to analytics is not consent to advertising.

In app analytics we use an analytics identifier assigned for the period of your consent and linked by Plenzo to your account. The data is pseudonymous: Plenzo can link the identifier to the account, so the data is not anonymous. We send events to PostHog after checking that consent is valid. We do not pass your account identifier or email address to PostHog. Each new consent period receives a new identifier and its history is not combined with earlier history.

9. Technical data and security

When you use the website and the app, we process technical data needed to handle the connection, including your IP address, and diagnostic information about the operation of the service and any errors that occur.

We use this data to ensure that Plenzo works correctly, to diagnose failures, to protect accounts against unauthorised access and to prevent abuse. The basis is our legitimate interest in ensuring the security and correct operation of Plenzo — Article 6(1)(f) GDPR.

Regardless of analytics consent, we record errors occurring on the website so that we know what has stopped working and can fix it. An error record includes technical information about the failure and about the device; we remove from it any address parameters and any content coming from fields you fill in, and we do not link it to your analytics profile. The basis is our legitimate interest in ensuring the correct operation of Plenzo — Article 6(1)(f) GDPR. We collect information about errors in the app only as part of the analytics described in section 8, if you have consented to it.

Regardless of analytics consent, the app retrieves feature configuration from Plenzo's server so that it knows which features to make available to you. Retrieving this configuration does not require an analytics or installation identifier and does not send PostHog information about your device or how you use Plenzo. The basis is our legitimate interest in the correct operation of the service — Article 6(1)(f) GDPR.

We limit the scope of data recorded in logs and apply safeguards against retaining unnecessary personal data and authentication data.

10. Notifications and biometrics

In order to send the notifications you have chosen regarding your finances and the operation of your account, we process the identifier used to deliver them, your notification settings and the content of the notifications. The basis is performance of the contract for the provision of Plenzo services — Article 6(1) (b) GDPR. Turning off push notifications does not prevent you from using the other features of the app.

We also use the device's time zone provided when registering for push notifications to schedule notifications for an appropriate time.

Delivery takes place through Apple services (Apple Push Notification service) on iOS and Google services (Firebase Cloud Messaging) on Android, to which we pass the identifier and the content of the notification. Some notifications contain information about your finances, including spending amounts, budget limits and the names of merchants or recurring payments. Depending on your device settings, the content may be visible on the lock screen. You can turn off individual notification categories in the app.

Marketing notifications, for example about offers, promotions or new features, are sent only on the basis of your separate, voluntary consent, which you can withdraw at any time in the app settings — Article 6(1) (a) GDPR and Article 398 of the Polish Electronic Communications Law. Notifications needed to operate your account and the service, including those about access expiring or synchronisation being suspended, are not marketing communication.

When you turn off all push notifications, we stop sending them and delete the device token. When you turn off only some categories, we retain the token and the settings of the categories that remain active. We delete the token and notification settings together with your account; we delete a token that stops working once we identify that state. We delete any residual data left after an unsuccessful operation within 30 days at the latest.

If you use biometric unlocking, the verification is carried out by your device's operating system. Plenzo receives only the authentication result, used locally to unlock the app. We do not receive biometric data and we do not transmit the authentication result to our servers.

11. Data recipients

To the extent needed to achieve the purposes described in this Policy, we use the following providers:

- Amazon Web Services — hosting, data storage and authentication. AWS also stores documentation and evidence of notices about changes to legal documents in a private, encrypted archive within the European Union.
- Tink AB — the account information service provider and data source described in section 4; a separate controller when providing that service, and a processor when storing and processing the data made available to us on our behalf;
- Resend — handling email communication;
- PostHog Inc. (PostHog EU Cloud) — analytics of website and app usage, depending on the consent given, and website error recording;

- Apple and Google — sign-in, handling purchases and subscriptions, and delivering notifications through the Apple Push Notification service and Firebase Cloud Messaging, depending on the platform and the features you use;
- Google — operation of Plenzo business email, where we correspond with you directly from our mailboxes;
- Meta Platforms Ireland Limited — joint controller of the statistical data of our Facebook and Instagram profiles, as described in section 2.

We may also disclose data to authorised public authorities where required by law.

12. Transfers outside the European Economic Area

Using our providers, including Resend and PostHog, may involve transferring data outside the European Economic Area, in particular to the United States. Storing analytics data in PostHog's European region does not exclude its processing outside the EEA in connection with the operation of the service.

Transfers take place on the basis of an adequacy decision or appropriate safeguards, in particular the standard contractual clauses approved by the European Commission.

You can obtain information about the safeguards applied to your data, and a copy of them, by contacting us at privacy@plenzo.app.

13. Retention periods

We retain analytics events while relying on valid consent to assess and improve use of the app or website, and only for as long as the data is needed for that purpose.

The event history available for analysis in PostHog depends on the current service plan. Under the Pro plan we use, that window is currently 7 years. This is the history window available in the tool, not an automatic data-deletion deadline.

After analytics consent is withdrawn, we delete the analytics profile and the data linked to it within 30 days at the latest; we may retain only data that is genuinely anonymised and aggregated. Deleting an account covers app analytics data, within the period described below for account deletion.

If previously granted app analytics consent has a specified end date, we do not extend it automatically. When that date is reached, we stop analytics and delete the profile and data for that completed period within 30 days at the latest.

Website analytics data is not linked to an account — we delete it after consent is withdrawn or expires on the website. The website analytics choice remains valid for up to 180 days, as described in the Cookies Policy.

We use limited pseudonymous technical telemetry solely for security, reliability and error diagnosis, and retain it for up to 30 days. We do not use it for product-usage analytics or to build a user profile.

We retain account data and financial data for as long as you use your account, unless you delete them earlier using the features available in the app. If you start registering but do not accept the Terms and confirm that you are 18 or over, no Plenzo account is created, and we delete the data provided or received at sign-in after 24 hours.

We keep your device's time-zone history only for the last 90 days; we delete anything older. We retain the time zone stored with a transaction, the time zone in your profile and a trip's time zone for as long as the transaction, account or trip they belong to.

You can request deletion of your account in the app or by writing to support@plenzo.app; we also handle a request for erasure of data that includes closing the account when it is sent to privacy@plenzo.app. A request made in the app is authenticated and we block access to the account immediately. For a request made outside the app, we first confirm that it comes from a person entitled to the account; where we have reasonable doubts, we ask for the information necessary to confirm this. Once a verified request is accepted, we block access to the account and delete the account data, financial data, bank connections and the app analytics data linked to the account from our active systems without undue delay, and no later than 30 days from receiving the request. For up to 48 hours after the process ends, we retain only the technical status of the operation, in order to confirm its result. We retain only the limited data necessary as documentation of the contract or of consent, or for handling a support matter, and data necessary to comply with a legal obligation or to establish, exercise or defend claims — for the periods described in this section.

After an account is deleted, we retain a hash of the user account identifier — the email address assigned to the account, regardless of the sign-in method — together with the date of the first registration of that account and the number of trial periods used, for no longer than 365 days from that registration. This allows us to recognise a new registration of the same user account and set the length of the trial period in accordance with the Terms. We delete this record when that period expires. The basis is our legitimate interest in preventing abuse of the trial period — Article 6(1)(f) GDPR.

Deleted data may remain for up to 14 days from its deletion from the active systems in secured backups that are not accessible in the ordinary service. If we restore a backup, we re-apply earlier deletions before the data becomes accessible.

In a separate deletion ledger, we keep only technical identifiers of deletions for up to 14 days so that, after restoring a backup, we can reapply the deletions before making the data available.

When disconnecting a bank, you can decide whether to keep previously retrieved transactions or delete them; deletion also covers attachments added to them. We retain your categorisation settings so that they work if you reconnect the bank; we delete them together with your account. In both cases we stop retrieving further data from that bank. Deleting the history from a bank does not cover your Plenzo account or data you entered independently of that connection. Disconnecting a bank does not by itself mean deleting your Plenzo account.

We retain correspondence concerning ordinary support requests, the requests themselves and their attachments for the time the matter is handled, and then for up to 6 months from its conclusion. We treat a matter as concluded once it has been closed or resolved. If we are waiting for your reply, we close the matter 30 days after our last message requiring a reply.

If you contact us after a matter has been closed, we create a new request. The previous matter is not reopened.

This cycle does not apply to formal consumer complaints or requests concerning your personal data. We handle complaints within the time required by law, generally within 14 days. We retain the complaint, correspondence about it and proof of delivery of our response for 7 years from the closure of the matter. We delete attachments provided in the matter, such as screenshots, 6 months after its closure, unless

they form the content of the complaint or response, or a legal obligation or ongoing dispute requires their retention.

We retain the content of a request concerning your personal data, correspondence about it and attachments provided for up to 24 months from the closure of the matter. We delete a full copy of data prepared solely to provide it to you at your request 30 days after it is provided, unless an ongoing complaint, supervisory complaint or dispute requires us to retain it.

We retain a minimal record of handling such a request — covering the type of request, dates, the result of identity verification, the outcome, and the date and method of response — for 7 years from the closure of the matter. This record is separate from the content of the request, correspondence and full copy of data.

We retain for longer only the data that is necessary to comply with a legal obligation or to establish, exercise or defend claims, for the period necessary for that purpose.

We retain documentation of consent given and withdrawn for the period the consent is relied on, and then for 7 years from its withdrawal. If consent has not been withdrawn, we count that period from the last event concerning it. We apply a shorter period where the need to comply with a legal obligation and to establish, exercise or defend claims ceases earlier. We delete the documentation of your decision concerning health data together with your account, and the documentation of consent to app analytics once deletion of the analytics data linked to the account has been confirmed.

We retain the record of conclusion of the newsletter contract — covering the email address, the accepted version and language of the Newsletter Terms, the date of acceptance, and the declaration that you are aged 18 or over — for the duration of the subscription, and then for 7 years from its end. This serves to demonstrate the terms on which the contract was concluded and to establish, exercise or defend claims. We apply a shorter period where the need for those purposes ceases earlier.

We retain the record of your acceptance of the Terms — covering the version accepted, the date, and the declaration that you are aged 18 or over — for the duration of the account contract, and then for 7 years from its end. This period covers the limitation period for claims and serves to demonstrate the terms on which the contract was concluded. We apply a shorter period where the need to establish, exercise or defend claims ceases earlier.

We retain evidence of notices about changes to legal documents for up to seven years after completion of the mailing, including retries. This may continue after an account has been deleted or a newsletter subscription has ended. We delete it earlier when it is no longer needed. We retain data for longer only where necessary to meet a legal obligation or for a specific dispute or proceeding, and only for as long as required for that purpose. We delete working recipient lists and reports from the application's database after checking that the archive is complete, normally 30 days after the mailing is closed.

14. Your rights

On the terms set out in the GDPR, you have the right to access your data and obtain a copy of it, to rectify it, to erase it, to restrict processing and to data portability.

Where we process data on the basis of legitimate interest, you may object on grounds relating to your particular situation. You may object at any time to processing for direct marketing purposes.

Where the basis for processing is consent, you may withdraw it at any time. This does not affect the lawfulness of processing carried out before the withdrawal.

To exercise your rights, contact us at privacy@plenzo.app. We will respond without undue delay and no later than one month from receiving the request. Where necessary, due to the complexity or number of requests, that period may be extended by a further two months; we will inform you of this and give the reason within the first month.

We process the data necessary to consider and fulfil requests and to document how they were handled, on the basis of a legal obligation — Article 6(1)(c) in conjunction with Articles 12–22 GDPR. If we have reasonable doubts about your identity, we may ask for additional information necessary to confirm it.

You also have the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych) or another competent supervisory authority, in particular in the country of your habitual residence, place of work or the alleged infringement.

15. Changes to this Policy

We update this Policy when the way we process data or the applicable law changes. We will inform you about significant changes in a manner appropriate to their scope, and about any new purpose of processing before processing for that purpose begins. If a change requires your consent, we will ask for it separately.

16. Language versions

This Policy is published in Polish and English. In the event of any discrepancy between the versions, the Polish version prevails.