CoinTrack Privacy Policy

Version: 1.0 Effective from: 1 November 2026

Service provider: Mikołaj Zienkowicz, ul. Długa 45A/2, 66-210 Zbąszynek, Poland, NIP (tax ID) 9271966162, REGON 388791452, e-mail contact@cointrack.pl, phone +48 881 583 586

This is an English translation of the Polish „Polityka prywatności CoinTrack". The Polish version is binding; in case of any discrepancy, the Polish version prevails.

1. In short

- Your data is controlled by **Mikołaj Zienkowicz**, running a sole proprietorship ("we").
- **Account data** (e-mail, name, sign-in method) is kept **separately from financial data** (budgets, expenses, assets). The financial database knows you only by an internal identifier (a pseudonym).
- Data is **encrypted in transit and at rest** (TLS and encryption by the infrastructure providers). The databases run in the Frankfurt region (Germany), with providers headquartered in the USA, under the safeguards required by the GDPR (section 12).
- **The AI Assistant (chat) runs on Google Cloud AI, called from our server. The AI model processes data in the European Union.** The conversation, receipt photos to be read and the Budget data needed for the answer go to Google. We store the chat history in the CoinTrack database, but **we do not store receipt photos**. Receipt Scanning requires your explicit consent (section 5). The Assistant can suggest entries, but only the ones you approve reach your budget.
- **Import from a CSV file** (Plus and Premium): your browser reads the file. Only the operations you approve reach your budget (section 8).
- **We do not train AI on your data.** We do not sell data. We do not use financial data for advertising.
- **Analytics** (PostHog) runs **only with your consent**. **E-mail marketing** - only with a separate consent.
- **Offline mode** (once available) is something you switch on yourself, separately on each device; it is off by default. Once you switch it on, the last fetched data of the Dashboard and the Budget and entries waiting to be sent are stored on that device, at most until you switch offline mode off or sign out (section 15).
- You have the right to access, rectify, erase and port (export) your data, to restrict processing, to object, to withdraw consent and to lodge a complaint with the President of the Polish Data Protection Office (UODO).

2. Controller and contact

Controller: **Mikołaj Zienkowicz**, running a sole proprietorship, ul. Długa 45A/2, 66-210 Zbąszynek, Poland, NIP (tax ID) 9271966162, REGON 388791452.

For personal data matters, write to **contact@cointrack.pl** or to ul. Długa 45A/2, 66-210 Zbąszynek, Poland. We have not appointed a data protection officer because we are not required to (Article 37 GDPR).

3. What data we process and where it comes from

Category	Examples	Source
Account data	e-mail address, whether it is verified, name, profile picture address from Google (stored with the account data, not displayed by the app), sign-in method (Google / e-mail link), sign-in sessions, account creation date, accepted document versions and consents	from you; name, e-mail and profile picture address - from Google if you sign in with Google
Family data	Family name, membership and roles (owner, member), invitations (who invited whom, status, expiry, when and in which language we sent the invitation message; for an invitation to an address that does not yet have an Account - the invitee's e-mail address in encrypted form and a cryptographic digest of it, in the account database, not in the financial database; the invitation link token - only as a hash; after further invitations are blocked - a digest of the address of the person who asked for it); for your membership - whether and when you hid the "Get started in 4 steps" list on the Dashboard (this applies only to you; other Members still see it)	from you and from other Family Members; the invitee's e-mail address - from the inviter (the Family's Owner)

Budget (financial) data	monthly budgets (amounts planned for expense categories in a given month), custom expense categories, income and expenses with their categories, recurring entries (name, amount, category, frequency) and the occurrences created from them, goals with deposits to and withdrawals from them, assets and liabilities with their value history, Tasks (row below), links between entries and imported items (amount, date, merchant and description from the import), entries suggested by the AI Assistant that you approved; for an entry saved in offline mode - a random key given by the device (with no content), which keeps the same entry from being saved twice (section 15)	from you and Family Members (the app creates the occurrences of recurring entries itself, following the rule you set); from imported files; from the Bank Feature (from the account information service provider)
Tasks (part of the Budget data)	title and note (e.g. the account number for a transfer, the transfer title, a link) - encrypted in the app (section 16.4); first due date and repetition; optionally an amount, a category, the way of payment (e.g. “save an expense when checked off”) and a link to a recurring entry; the due dates something happened to (checked off, moved, skipped, deleted), and for a check-off - the date and time, how (by hand or from an import), the pseudonym of the person who checked it off (never an e-mail or name), and the link to the expense saved on check-off or to the imported item; for imports - the payee from the import remembered for the Task (encrypted) and the Task–imported item pairs you rejected (“Not this one”), stored with the imported item’s identifier, without its content (section 8)	from you and Family Members; the app works out the following due dates from the repetition you set; the payee - from the import

Conversations with the AI Assistant	content of your messages and the Assistant's answers; we do not store receipt photos (section 5); record of changes made in the chat (section 5(4))	from you; answers - generated by the Google Gemini model
Receipt Scanning	the receipt photo - only for the time of the read, not stored; the result of the read (date, amount, shop, items) in the "To approve" queue; your consent to the processing of specially protected data (date and time, wording of the consent, any withdrawal)	from you; the result of the read - generated by the Google Gemini model
Import data (section 8)	operations from the CSV file that you select for import: date, amount, merchant or counterparty and description of the operation (the description may include counterparties' data) and the operation fingerprint (a hash); the file column layout remembered for the Family; categories remembered for merchants; operations you skip or reject stay in the import queue with the same data (section 8.6)	from you, from a file downloaded from your online banking

Billing data	Przelewy24 order and payment IDs, the payment method (BLIK, transfer, card), Plan, Plan Period, amounts, payment and refund status, the amount of a referral programme Discount used in the order, the country of residence stated with the order (sales only in the EU, VAT/OSS) and the country determined from the IP address at the time of the order (without the IP address itself) - as a second piece of evidence of the place of residence for VAT (Article 24f of Regulation 282/2011); for a refund by bank transfer to an account you indicate (Terms § 10(4)) - that account number and the account holder's name; at Przelewy24: e-mail address, order amount and description, payment country and language, IP address and the payment details you give directly to Przelewy24 or to your bank (e.g. card details, the account and account holder details for a transfer); only for an invoice on request - name or company, address, tax ID	from you and from Przelewy24; we determine the country from the IP address ourselves at the time of the order, through our hosting provider (Vercel Inc., section 11)

Data from the form of a withdrawal from the contract or a refund request	full name (in the app filled in from your account data, you can change it), a note and an extra e-mail address for a copy of the confirmation (both optional). We do not store them in the database: they go only into the confirmation e-mail and its copy, and the full name and the note also into the notice of the statement we receive at contact@cointrack.pl. The register of statements keeps the contract, the kind of statement, how it was made, the date and time it was received and, for a statement sent by e-mail or post, also the date (and time, if known) it was sent, the refund amount and a reference to the payer (a digest and a ciphertext of an identifier, without an e-mail). If the statement came by e-mail or post, we also send the confirmation once to the address you wrote from or gave in your letter, and if you no longer have an Account - only to that address. We do not store that address in the register or in the app's logs and do not retry sending to it; it passes through Resend, which sends the confirmation (section 11), and stays in our correspondence with you.	from you
Trial control data	a cryptographic digest (HMAC) of the e-mail address of the person who started the Trial - without the address itself - the date the Family's Trial started and the date the digest was recorded	generated when a Trial starts

Referral programme data	the referral code (link) assigned to the Account; pseudonymous identifiers of the referrer's Account and of the referred person's Account (without e-mail addresses); the referral status and its dates (Account creation, payment, grant or refusal of the Discount); Discounts granted, their expiry date and use (the order and the Discount amount). To check whether the referred person's Account is new, we use the e-mail digest for Trial control (without the address itself)	generated when you or a person you referred take part in the referral programme. The referrer sees the status of the referral (waiting for 14 days to pass - with the date the Discount will be granted - or counted), without your e-mail, Plan or amounts
Connected AI apps data	token hash, scope, expiry date, usage log (date, tool, result)	generated when you use the feature
Technical and security data	IP address, browser/device type, server and error logs, feature usage counters (without content), the AI usage log (type of feature, model, number of tokens, cost, number of items, result - without content, section 5)	from your device, automatically
Analytics data (only with consent)	page views, clicks, in-app events (e.g. "budget created"), without amounts or transaction descriptions	from your device, with consent
Correspondence	content of messages, complaints and GDPR requests; for messages to contact@cointrack.pl also the sender's address and name, attachments and headers; a bank account number and the account holder's name, if you give them for a refund by transfer (Terms § 10(4))	from you

People invited to a Family (Article 14 GDPR). If someone invited you to a Family, we received your e-mail address from the inviter, the Owner of that Family (Article 14(2)(f) GDPR). We send the invitation message to that address. In that message, at the first contact (Article 14(3)(b) GDPR), we say who the controller is, where we got the address, for what purpose and on what basis we process it, how long we keep it, who we entrust it to and what your rights are, including the right to object. Details: section 7(2).

Other people's data (Article 14 GDPR). Transaction descriptions from imports or the bank may contain third parties' data (e.g. the sender of a transfer), and so may the names of entries and the notes of Tasks that you or Family Members type in (e.g. a landlord's account number). We use it solely to keep the budget of the Family that entered or imported it. In the Bank Feature we remove such

data before saving. Informing each such person individually would be impossible or would involve a disproportionate effort (Article 14(5)(b) GDPR), so we publish this information instead.

We do not want special categories of data. Expenses can sometimes reveal, for example, information about health or beliefs. We do not automatically create categories or draw conclusions about such information and do not use it for any purpose other than keeping your budget. Categories you create yourself remain yours. Please do not enter health data in expense descriptions or in conversations with the AI Assistant. During import we do not send to AI operations whose description points to such data (section 8). **Exception: Receipt Scanning.** A receipt (e.g. from a pharmacy) may reveal health data or other specially protected data. That is why we process a receipt photo only with your explicit consent (Article 9(2)(a) GDPR, section 5).

4. Purposes, legal bases and retention periods

Purpose	Legal basis (GDPR)	How long
Creating and running the Account, sign-in, providing CoinTrack services (budget, Tasks, Family, AI Assistant, file import, copy of your data)	contract - Article 6(1)(b)	until the Account is deleted; Tasks with their check-off history belong to the Family - until the Task is deleted with its history, or the Family or the Account of its only Member is deleted (section 7.5); then up to 31 days in backups (section 10)

Family invitations: checking whether the address can join, sending the invitation message (also to a person without an Account), resending and cancelling by the Owner, confirmation or refusal by the invited person, showing the Owner the invitation's status (section 7(2))	for the invited person, until the invitation is accepted - legitimate interest, Article 6(1)(f). The inviter has an interest in inviting a person they chose to a shared budget, and we have an interest in delivering the invitation without revealing whether the address has an Account and in preventing abuse. After acceptance - contract, (b). For the inviter - contract, (b). Blocking further invitations after an objection - legitimate interest, Article 6(1)(f): respecting the objection and not sending further invitations	the invitee's encrypted address and its digest: deleted immediately on acceptance (the address then remains only as the account data of the person who joined); after refusal, cancellation or expiry, kept for 30 more days and then deleted (backups - up to 31 days, section 10). During those 30 days the inviter sees the invitation's status with a masked address (e.g. a***@example.com), and we can look into a report of an unwanted invitation or abuse. After an objection - deleted without undue delay. The hash of the link token - until the invitation is accepted, refused, cancelled or expires. The invitation record in the financial database (who invited, to which Family, status, expiry - without the invitee's address) - until the Family, the inviter's Account or the invited person's Account is deleted. Block on further invitations (after clicking "I don't want invitations" or at your request after an objection): a separate record in the account database - only a digest of the address, not the address itself - until the block is withdrawn. To withdraw it, write to contact@cointrack.pl from the address it concerns.
File import: recognising the file layout, checking for duplicates, matching with your entries and Tasks, the "To approve" queue, category suggestions - also from AI unless you turn them off (section 8)	contract - (b)	like other Budget data: until you delete it, at the latest until the Account is deleted (backups expire within 31 days); skipped and rejected operations - until the Family is deleted (section 8.6); data for checking duplicates of operations you do not select for import - we do not store it
Receipt Scanning: reading the receipt photo and suggesting an entry (section 5)	contract - (b); for special categories of data visible on the receipt - your explicit consent, Article 9(2)(a)	the photo - only for the time of the read, we do not store it; the result of the read and approved entries - like other Budget data

AI usage log: counting limits, controlling AI costs and detecting abuse (section 5)	contract - (b) (Plan limits); legitimate interest - (f) (cost control, preventing abuse)	13 months from the record; earlier - together with the deletion of the Family
Offline mode, once you switch it on on a device: storing on that device the last fetched data of the Dashboard and the Budget and the entries waiting to be sent (section 15)	contract - Article 6(1)(b); storing on and reading from the device without consent in the cookie banner, because they are necessary for the feature you switched on to work (Article 399(3)(2) of the Polish Electronic Communications Law)	on the device: an entry - until it is sent; the Dashboard and Budget data - until the next fetch, at most 30 days; everything - at most until you switch offline mode off, sign out, open the app after the session has expired, switch the Family or delete the site data
Handling paid Plans, the Trial, limits, payments via Przelewy24, extensions, withdrawals and refunds	contract - Article 6(1)(b)	for the term of the contract, then until claims become time-barred; the register of statements (withdrawals from the contract and refund requests): until 31 December of the sixth year after the year in which the refund deadline passed or, if a dispute is pending, until it ends
Issuing invoices, bookkeeping, VAT settlement	legal obligation - Article 6(1)(c) (VAT Act, Tax Ordinance, Accounting Act)	5 years from the end of the calendar year in which the tax payment deadline passed (Article 86 § 1 read with Article 70 § 1 of the Tax Ordinance)
VAT records for sales to consumers in other EU countries (OSS scheme) - applies when we settle VAT under the OSS scheme: country of residence and the evidence used to determine it (declaration, country from the IP address), date, amount, VAT rate	legal obligation - point (c)	10 years from the end of the year in which the sale was made (Article 369k of Directive 2006/112/EC)
Referral programme: assigning the referral, checking the conditions and exclusions, granting, returning and settling Discounts (Terms § 8(13))	contract - Article 6(1)(b); checking the exclusions and preventing abuse (e.g. referring yourself) - legitimate interest, (f)	until the referral is settled and the Discounts are used or expire

Defending against claims concerning the referral programme	legitimate interest - (f)	until 31 December of the sixth year after the year in which the referral was finally settled (Discount used, expired or refused) - Article 118 of the Civil Code; also after the Account is deleted. The amount of a Discount used in a purchase is part of the payment documents and we keep it for 5 years like invoices
Service messages (sign-in link, contract and payment confirmations, notices of a failed payment, reminders of the end of the Plan Period, withdrawal confirmations, notices of the grant, refusal, return and expiry of a referral programme Discount, notices of a Family handover, takeover and scheduled deletion, document changes, security alerts)	contract - (b); legal obligation - (c) (information required by the Consumer Rights Act)	for the term of the contract
Handling complaints, replying to messages	contract - (b); legal obligation - (c); our legitimate interest - (f) (communication)	until the matter is closed, then until claims become time-barred (mail to contact@ - periods in the row below)

Keeping mail sent to contact@cointrack.pl and our replies	as for the matter the message concerns: contract - (b); legal obligation - (c); our legitimate interest - (f) (communication, establishing, pursuing and defending claims)	(a) a statement of withdrawal or a refund request and the correspondence about it (including a bank account number for the refund) - until 31 December of the sixth year after the year in which the refund deadline passed; (b) complaints and other correspondence about the contract - until 31 December of the sixth year after the year in which the contract ended or, if later, the matter was closed; (c) GDPR requests and our replies - until 31 December of the third year after the year in which we closed the matter; (d) other messages - 12 months after the last message in the thread; spam and phishing are deleted at once, at the latest after 30 days. If a dispute or proceedings are pending, the related messages are kept until they end and, after a final judgment, until the claim it confirms becomes time-barred. We do not archive attachments larger than 30 MB - Resend deletes them after 30 days.
Handling GDPR requests (accountability)	legal obligation - (c) (Article 5(2), Article 7(1) GDPR)	consent record - for the duration of the consent and until claims become time-barred (generally up to 6 years); a GDPR request and our reply - until 31 December of the third year after the year in which we closed the matter

Evidence of consents in the consent register: a cookie banner choice (also when saved with the Account), acceptances of the Terms of Service, confirmations of having read the Privacy Policy, statements made when buying a Plan (acceptance of the Terms of Service, the request to start the Plan before the 14 days to withdraw from the contract are over, the confirmation that "coming soon" features are not part of the Plan), the consent to the processing of special categories of data for Receipt Scanning and its withdrawal, the consent to marketing e-mails and its withdrawal	legitimate interest - (f) (defending against claims and accountability, Article 5(2) and Article 7(1) GDPR)	cookie banner choice: 3 years from the consent expiring or being withdrawn; acceptances of the Terms of Service, confirmations of having read the Privacy Policy and consents given when buying: 6 years from the end of the contract (Article 118 of the Civil Code), that is from the deletion of the Account, and for consents given when buying from the end of the paid Plan Period if it still runs after the Account is deleted (counted as the deletion of the Account plus 12 months); a consent given when buying recorded without an Account: 7 years from when it was given (12 months and 6 years); the Receipt Scanning consent and the consent to marketing e-mails: 3 years from their withdrawal or from the deletion of the Account; entries past their period are deleted once a day
Security, abuse prevention (e.g. repeated Trials), logs	legitimate interest - (f)	server logs (function logs at Vercel): up to 1 day; security logs: 12 months; AI Assistant abuse-protection counters - up to 2 days; the daily Family invitation counter (Family, inviter’s pseudonym, day, count - no e-mail address; Terms § 9(10)) - up to 2 days; e-mail digest for Trial control (also used to check whether the referred person’s Account is new - Terms § 8(13)): 24 months from when it was recorded, also after the Account is deleted (after that the same e-mail can start a Trial again), digests past their period are deleted once a day
Establishing, pursuing and defending claims	legitimate interest - (f)	until claims become time-barred (generally 6 years, 3 years for periodic benefits - Article 118 of the Civil Code)
Product and website analytics (PostHog)	consent - (a); access to the device - consent under Article 399 of the Electronic Communications Law	until consent is withdrawn; PostHog events are kept for 12 months

E-mail marketing (newsletter, offers)	consent - (a) and consent under Article 398 of the Electronic Communications Law	until consent is withdrawn

Providing account data is voluntary, but without it you cannot create an Account. Providing invoice data is necessary if you want an invoice. Consents to analytics and marketing are entirely voluntary - CoinTrack works the same without them. The Receipt Scanning consent is also voluntary: without it you cannot scan a receipt, but all other features work the same.

5. AI Assistant (chat) and Receipt Scanning

1. The in-app **AI Assistant**, including reading a receipt from a photo, runs on **Google Cloud AI** (Gemini Enterprise Agent Platform, formerly Vertex AI), in the “eu” location (Terms of Service § 13) - the AI model processes data in the European Union. The request to Google is sent by our server, not by your browser (AI information - Annex 3 to the Terms of Service). The same service is used by Receipt Scanning (the “Scan a receipt” screen or a photo attached in the chat) and by category suggestions during import (section 8).
2. We send to Google: the conversation, a receipt photo to be read and the Family’s Budget data needed for the answer (e.g. income, expenses, assets, goals, the Family name). From Tasks, we send the amounts planned in a given month, as part of the total of planned expenses, and, when the AI Assistant needs them to answer (e.g. you ask about Tasks or ask it to change a Task), also the titles, due dates, amounts, repeat settings and status of Tasks. An expense saved when you check off a Task is named after the Task's title and is sent to Google like any other expense. **We never send Task notes. We do not send your e-mail or name.**
3. Google processes this data as our processor (Article 28 GDPR), under the Google Cloud data-processing addendum (Cloud Data Processing Addendum), only on our instructions and only to provide the service to us and to secure it. **Google does not use it to train AI models** or for its own purposes. Google does not keep prompts and answers longer than needed to answer. Exceptions:
    1. **abuse monitoring** - if Google’s automatic safety filters flag a possible breach of the service’s usage policies, Google may store the prompt solely to check whether a breach occurred. Such a record may be reviewed by a Google employee. Google keeps it for up to 90 days, in the EU;
    2. **cache** - to answer faster, Google may by default keep fragments of our project’s prompts in a cache, in the EU, for up to 24 hours. This is a mechanism of Google’s service; we do not ourselves store any content in it. No one outside our project has access to it.

    Transfers outside the EEA and recipients are described in sections 11 and 12.
4. **We store conversation history in the CoinTrack database** (financial database, Neon, Frankfurt): your messages, the Assistant’s replies, the budget data the Assistant read in order to answer, and the cards with proposed entries and their status (e.g. approved). Separately, we store the record of changes made in the chat: what the Assistant proposed, the data before and after the change, the status of the proposal and when you approved or undid it. The record lets you undo a change and helps us handle your request; we encrypt it like the conversation itself (section 16.4). The history and the record are linked to your pseudonym. We delete the conversation and its record when you click “New conversation”, and at the latest when the Account is deleted (section 10). Deleting a Family deletes the record of changes to its data. Messages with data of a Family you left, were

removed from or that was deleted stay in your conversation until you click “New conversation” or delete your Account. Backups are described in section 10. The legal basis is the contract (Article 6(1)(b) GDPR). We are the controller of this data.

5. **We do not store receipt photos.** After the read we delete the photo from our server’s memory. The rest of the conversation, described in paragraph 4, stays in the conversation history (e.g. the answer that the receipt is waiting in the “To approve” queue) - without the photo and without a marker that it was attached. That is also why photos are not in the “Download my data” copy of your data (section 17).
6. **Consent to Receipt Scanning.** A receipt may reveal data about your health (e.g. pharmacy purchases) or other specially protected data (Article 9 GDPR), also about people close to you. That is why we ask for your explicit consent before the first scan (Article 9(2)(a) GDPR; Terms of Service § 13(8)). You give it once, for your Account. You can withdraw it at any time in Settings → Privacy. Withdrawal does not affect the lawfulness of earlier reads. Entries you have already approved and suggestions waiting in the “To approve” queue stay - you still decide about each of them. Without the consent you cannot scan another receipt. We record the consent and its withdrawal in the consent register (section 4).
7. **AI usage log.** Each time AI is used (a message, a scan, category suggestions during import) we record for the Family: the type of feature, the model, the number of tokens, the cost, the number of items and whether it succeeded - without content. We need it to count limits (Terms of Service § 9), control costs and detect abuse. We keep it for 13 months, and delete it earlier together with the Family.
8. The AI Assistant can suggest entries (e.g. an expense from a receipt). Only **entries you approve** reach your budget, just like a manual entry. From then on they are Budget data as described in section 3.

6. Signing in with Google or an e-mail link

1. You can sign in with **Google** or with an **e-mail link** (magic link, no password). We do not offer password sign-in. Both lead to the same Account if you use the same e-mail address.
2. When you sign in with Google, we receive from Google your e-mail address, whether it is verified, your name and your profile picture address. The picture address is stored with the account data, but the app does not display it - it shows your initials instead. **Google learns that you use CoinTrack and sign in to it.** Google processes this data as a separate controller under its privacy policy (https://policies.google.com/privacy). If you do not want that, sign in with an e-mail link - Google then takes no part in the sign-in.
3. Sign-in is handled by Neon Auth (Neon’s authentication service), in the account database in the Frankfurt region. Neon Auth sends sign-in links through Resend from no-reply@cointrack.pl.
4. Sign-in data and account data are in a separate database from Budget data, with separate access credentials.

7. Family

1. A Family’s Budget data can be seen and changed by all its Members according to their roles. Members also see your name and e-mail (instead of a profile picture, the app shows initials). Every

Family Member can download the Family's income and expenses to a file, including entries added by other Members (descriptions, amounts, categories). The file does not contain names or e-mail addresses. Once downloaded, the file is on that person's device, and they are responsible for what they do with it.

2. **Invitations.** A Family's Owner invites people by entering the invitee's e-mail address. We do not tell the inviter whether that address has an Account. If the address can join, we send a service message with the invitation to it through Resend (section 11), with a single-use link valid for 7 days from the latest sending. A person who has an Account also sees the invitation in the app. The Owner can resend the invitation (no more often than every 15 minutes; the new link replaces the previous one) or cancel it. A daily invitation limit applies (Terms § 9(10)). The message gives the inviter's name as saved in their Account. If there is no name, we write in general terms, without the inviter's e-mail address. We do not include the Family name or any Budget data. The message is not advertising and contains no promotional content. If it cannot be sent, we do not save the invitation.

   We do not store the invitee's address in the financial database. When the address does not yet have an Account, we keep the address in encrypted form and a cryptographic digest of it in the account database, and the link token only as a hash. The inviter sees the invitation on the sent list with a masked address (e.g. a***@example.com). The invited person joins only after they sign in with the invited address (or create an Account and accept the Terms) and confirm the invitation. We then delete the address record kept with the invitation, and the address remains as their account data. After the invitation is refused, cancelled or expires, we keep the address record for 30 more days (section 4) and then delete it. Deleting the inviter's Account or the Family cancels its invitations and deletes the address record. Until acceptance, the basis is the legitimate interest of the inviter and of us (Article 6(1)(f) - described in section 4); after acceptance, the contract (point (b)).

   If you received an invitation you do not want, you do not have to do anything - it will expire on its own. **You have the right to object** (Article 21 GDPR): click "I don't want invitations" in the message, reply to it or write to contact@cointrack.pl. We will then cancel the invitation and delete your address. Clicking "I don't want invitations" also blocks further invitations to this address straight away; if you write to us, we will block them at your request. To make the block work, we will keep only a digest of the address (not the address itself) until you withdraw the request (by writing to contact@cointrack.pl).

3. The Owner of a Family that has other Members can hand it over to another Member (Settings → the family profile card → "Hand over"). The new Owner gets an e-mail about it. If the Owner deletes their Account without a handover, the Family stays without an Owner for **14 days**. Its Members get an e-mail with the deadline and see a notice in the app, can download their data (section 17), and any of them can take the Family over ("Take over"). After a takeover the Family stays, and the other Members get an e-mail about it. If nobody takes it over, after 14 days we delete the Family together with its Budget data. Until then the Family's Budget data, including data entered by the former Owner, stays available to its Members. The basis is the contract with each Member (Article 6(1)(b)).

4. The Family name is visible to all Members. Please do not use a surname in it.

5. **Tasks** belong to the Family. All its Members see the Tasks and their check-offs and can add, change and check them off. On a check-off we store the pseudonym of the person who checked

off the due date - never an e-mail or name. The app does not show it, and in the copy of your data (section 17) we mark only which check-offs are yours. If you delete your Account, the check-off stays in the Family without information on who made it. “End the task” stops future due dates, and the check-off history, with its title, stays in “Done”. “Delete the task with its history” permanently deletes the Task, its note and its check-off history for the whole Family; expenses saved on check-off stay in the budget. You delete a single check-off in “Done” (“Delete the entry”); its expense also stays in the budget. We keep Tasks with their check-off history until the Task is deleted with its history, or the Family or the Account of its only Member is deleted (section 4). Data disappears from backups after 31 days at the latest (section 10).

8. File import

1. On the Plus and Premium Plans you can import operations from a CSV file downloaded from online banking (Terms of Service § 11). **Your browser reads the file.** The file itself does not reach our server and we do not store it. Import does not connect to your bank. We do not store logins or passwords to online banking.
2. We send to our server only what is needed at the later steps of the import:
    1. **recognising the file layout** - the column names from the file header (without account numbers). We remember the column layout you confirm for the Family (encrypted, section 16.4), so that we do not ask you again at the next import;
    2. **checking for duplicates** - the booking date, amount and reference number of each operation (and when an operation has no reference number - a sequence number that the app gives it among operations from the same day with the same amount). Our server calculates an operation fingerprint (a hash) from them and compares it with the fingerprints of operations imported earlier. For operations you do not select for import we store nothing;
    3. **the operations you select for import** - the date, amount, merchant or counterparty and description. They go to the “To approve” queue together with the operation fingerprint; we do not store the reference number itself.
3. **Matching with your entries.** Our server, without AI, compares operations with the entries you already have in the budget, so that the same expense does not reach the budget twice. We treat as similar: for a recurring entry - an amount within 10% and a date within 5 days; for a one-off entry - an amount within PLN 1 and a date within 2 days. When the operation is a charge in a foreign currency converted into złoty, both amount thresholds are replaced by one: an amount in złoty within 3%. We compare a receipt waiting in the “To approve” queue with an operation from the file by the day the card payment was made, if the file gives it, and not by the booking day (the booking day remains the operation’s date in the budget). We suggest the link; you decide.
4. **Matching with Tasks.** If you tick “Recognise in the bank import” for a Task, we compare imported transactions - from a file or from the Bank Feature (section 9) - with that Task’s due dates: the transaction’s amount and date with the Task’s amount and due date, and the transaction’s merchant and description with the Task’s title and remembered payee. Our server does the comparison, without AI and without passing data to anyone else. A due date is checked off only once you approve the transaction in the “To approve” queue, and when the match is uncertain we ask you (“Check off the task” / “Not this one”). After a check-off from an import we remember the payee from the transaction with the Task (encrypted, section 16.4), and after “Not this one” - that this pair does not match, so that we do not suggest it again. We delete this data together with the

Family.

5. **Category suggestions from AI.** Unless you turn off “Suggest categories with AI” (on by default), the AI model (section 5) suggests a category for an operation we do not know from your earlier choices. We send to Google only: the cleaned merchant name and operation description (without account numbers), the type of operation (e.g. card payment, transfer), the direction (incoming or outgoing) and the names of your Family’s categories, including custom ones. **We do not send** amounts, dates, reference numbers, transfers to and from private individuals (e.g. BLIK to a phone) or operations whose description contains words pointing to specially protected data (e.g. about health or religion). We label the suggestion “AI suggestion” and you can change it before approving. The legal basis is the contract (Article 6(1)(b)) - it is part of the import service, which you can turn off on the import screen. We remember the category you approve for that merchant (encrypted, section 16.4), so that next time we can suggest it without AI.
6. **Only what you approve reaches the budget.** Approved operations become Budget data (section 3). Operations you skip or reject are not added to the budget, but they stay in the import queue as skipped or rejected: with the date, amount, merchant or counterparty, description and operation fingerprint. This way the same operation does not come back to the queue when you import a file that contains it. We encrypt the merchant and description in the app (section 16.4), and the whole database is encrypted by its provider (section 16.1). We keep them until the Family is deleted - a Family in which you are the only Member is deleted together with your Account (section 10) - and they disappear from backups within 31 days at the latest. The legal basis is the contract (Article 6(1)(b) GDPR). If you want us to delete them earlier, write to contact@cointrack.pl (Article 17 GDPR).
7. **How long:** we keep approved operations like other Budget data: until you delete them, at the latest until the Account is deleted (backups expire within 31 days). Skipped and rejected operations - until the Family is deleted (paragraph 6).

9. Bank Feature

The Bank Feature is in preparation and we do not process any data in it at present. This section applies from the day it becomes available.

1. The account information service is provided by a licensed provider (the AIS Provider), whose name and registration details we will show in the app before you connect an account, under a separate agreement with you. That provider is a **separate controller** of the data retrieved from the bank and informs you about it in its own privacy notice, which you will see before you connect an account.
2. From the provider, on your instruction, we receive: the list of accounts (name, currency, balance), transactions (amount, date, description, identifier), the status and expiry date of the consent. **We do not receive your bank login credentials.**
3. Before saving, we remove other people’s personal data from descriptions (names, surnames, account numbers, phone numbers, addresses). We save the amount, date, a short description, the category and a pseudonymous transaction identifier.
4. We keep Bank Feature data until you disconnect the account with the “Disconnect and delete data” option or delete your Account. We keep the Bank Feature security event log for 12 months.
5. Transaction categorisation is automatic (profiling, section 13).

10. Account deletion and periods after deletion

1. You can delete your Account in Settings → “Delete account”.
2. When the Account is deleted, we **immediately** delete: the account data together with sign-in methods and sessions, the link between the Account and the financial data, the chat history with the AI Assistant, and the Families in which you are the only Member, with their Budget data. You leave Families that other people belong to, and their Budget data stays. If you owned such a Family, it stays for up to 14 days for another Member to take over; if nobody does, we delete it after that deadline (section 7.3). If you delete your Account and you paid for your Family’s Plan, the Plan keeps running if the Family stays (it has other Members or someone takes it over). If the Family is deleted, the Plan contract expires and we refund an extension that has not started (Terms § 19(4)). We keep the data of that contract and payment (without your e-mail and name) for the periods in section 4, including until the refund is made. If, when the Account is deleted, the 14 days to withdraw from the contract or the refund guarantee period are still running or ended less than 30 days earlier, we keep that contract's data (without your e-mail and name) until 30 days after that period ends - so that we can accept a statement sent by e-mail or post before the end of the period that reaches us later, and make the refund. We do not save cards or other payment methods, so after the Account is deleted there is nothing to charge. We also delete your PostHog profile (if you consented to analytics). We delete the offline mode data from the device on which you delete the Account; on other devices - the next time CoinTrack is opened on them, and before that you can delete it by switching offline mode off or deleting the site data there (section 15).
3. **Backups.** Database backups are kept by the provider for up to **31 days** and are then deleted automatically. Data deleted from your account disappears from the backups no later than that. The copies are encrypted by the provider and we use them only to restore the system after a failure. If we restore the system from a backup, we will delete your data again. The backups are stored in the European Union or, if outside it, on the basis of the EU–US Data Privacy Framework or standard contractual clauses (section 12).
4. Google keeps an AI Assistant prompt only when its automatic filters flag possible abuse - for up to 90 days, solely to check the breach. Google’s service deletes the cache within 24 hours at the latest (section 5).
5. We keep only data required by law (e.g. invoices and payment data held by us and the accounting office - 5 years, section 4) or needed to defend against claims (e.g. confirmations of purchase, refund, consents) - until claims become time-barred (register of statements - section 4); section 4 gives the periods for the consent register. We keep the e-mail digest for Trial control (without the address itself) for 24 months from when it was recorded, also after the Account is deleted (section 4). PayPro S.A. (Przelewy24) keeps the data of your payments as a separate controller for the period required by its legal obligations (section 11), also after the Account is deleted. We keep referral programme data (without e-mail addresses) after the Account is deleted until the end of the period in section 4.

11. Who we share data with (recipients)

We use providers that process data on our behalf (processors, Article 28 GDPR) and entities that are separate controllers.

Entity	Role	Purpose	Where it processes	Basis for transfers outside the EEA

Vercel Inc. (USA)	processor	hosting of the app and website, server functions (all app data passes through them), logs, website performance measurement (Speed Insights, not tied to a person)	server functions in the fra1 region (Frankfurt); access and edge network also in the USA	EU–US Data Privacy Framework (DPF), with standard contractual clauses (SCC) from Vercel's data processing agreement as a fallback
Neon (Databricks, Inc., USA)	processor	databases (separately: account/ sign-in and financial data, including the AI Assistant chat history), Neon Auth sign-in service, backups; archive of mail sent to contact @cointrack.pl and our replies (section 3 "Correspondence"), for the periods in section 4	AWS, Frankfurt region (Germany); service access possible from the USA; Neon's own copies in the EU or transferred on the basis of the DPF or SCC	DPF (Databricks, Inc. including Neon, LLC), with SCC from the Databricks data processing agreement as a fallback

Resend (Plus Five Five, Inc., USA)	processor	sending sign-in link e-mails (Neon Auth mail server), Family e-mails (handover, the Owner's account deletion with the Family's deletion date, takeover; without the Family name), Family invitation e-mails, also to people who do not have an Account (the invitee's address, the inviter's name if saved in their Account, the expiry and the link with the token; without the Family name or Budget data) and, from the launch of payments, the transactional e-mails of a paid Plan: contract confirmation, payment confirmations, payment problems, reminders of the end of the Plan Period, confirmations of a withdrawal or a refund request and notices about referral programme Discounts; Resend receives your e-mail address, your name and the contract data in the message (Plan, period, amounts, dates, order and payment numbers, payment method - never the card or account

	number), and for a withdrawal from the contract or a refund request also the full name and the note from the form and an extra e-mail address if you give one for a copy of the confirmation; Resend also receives messages sent to contact@cointrack.pl (the sender's address and name, content, attachments, headers) - including statements of withdrawal and replies with a bank account number for a refund by transfer - and sends the confirmation of a statement made by e-mail or post to the address you sent it from or gave in your letter	mail sent and received in the EU region (Ireland); message content (including mail to contact@) and logs stored in the USA, at Resend for up to 30 days	SCC from Resend's data processing agreement; Resend also participates in the DPF (active status, with re-certification under review)

PayPro S.A., operator of Przelewy24, ul. Pastelowa 8, 60-198 Poznań, Poland, KRS 0000347935, NIP 7792369887 - a domestic payment institution (KNF, no. IP24/2014)	separate controller - processes data to carry out payments and to meet its own legal obligations (including anti-money laundering and counter-terrorist financing, fraud prevention and handling payment complaints)	When you buy a paid Plan (BLIK, fast bank transfer or card): we pass PayPro your e-mail address, the amount, currency, description and ID of the order, and the payment country and language. PayPro receives card details, account details and your IP address directly from you or your bank - we do not see them. We do not ask PayPro to save your card. Our basis for passing the data on: the contract (Article 6(1)(b) GDPR). PayPro's bases: as set out in its information notice - including a legal obligation (point (c)) and legitimate interest (point (f)). PayPro keeps payment data for the time the payment service is provided and 13 months from the debit of the account (or from the day the payment was to be made), and then for the period required by law (payment service documents at least 5 years, AML data 5 years). PayPro may also process other data, e.g. to verify identity. Details: Przelewy24 GDPR

information notice for payers; PayPro's data protection officer: iod@przelewy24.pl	Poland (EEA)	not applicable - PayPro states that it does not intend to transfer data outside the EEA

PostHog Inc. (USA) - only with consent	processor	product and website analytics	PostHog EU Cloud (Frankfurt); service access possible from the USA	DPF and SCC
Google Ireland Limited (Ireland) / Google LLC (USA)	separate controller (Google sign-in)	Google sign-in, only if you choose it: Google passes us your e-mail, name and profile picture address and learns that you use CoinTrack (section 6)	EU and USA	DPF (Google LLC)
Google (Google Cloud) - Google Cloud AI (Vertex AI)	processor	AI Assistant answers, Receipt Scanning and category suggestions during import, called from our server: the conversation, receipt photos to be read (we do not store them), the Budget data needed for the answer (including Task titles and due dates, without their notes) and, for imports, cleaned merchant names and operation descriptions (section 8), without e-mail or name; Google does not use them to train AI models or for its own purposes; it stores a prompt only when filters flag possible abuse - for up to 90 days (section 5)	the AI model processes data in the EU (“eu” location), where abuse-monitoring records are also kept; service access and abuse review are also possible from outside the EEA	standard contractual clauses (SCC) from the Google Cloud data-processing addendum and, where applicable, also the EU–US Data Privacy Framework (DPF)

Google Cloud KMS (Google Cloud)	processor	encryption key management (only keys reach KMS, not your data)	Germany (Frankfurt)	standard contractual clauses (SCC) from the Google Cloud data-processing addendum and, where applicable, also the DPF
Biuro Rachunkowe Paulina Budzicka (Wawelska 1, Przyprostynia, 64-360 Zbąszyń, Poland, NIP 7881999696)	processor	bookkeeping, invoices	Poland	not applicable
Members of your Family	-	shared budget	-	-
The referrer (if you created your Account from a referral link)	-	the status of the referral (waiting for 14 days to pass - with the date the Discount will be granted - or counted), without your e-mail, Plan or amounts	-	-
Public authorities	separate controllers	only where required by law	-	-

We keep the current list of providers in this policy and inform you about changes.

12. Transfers of data outside the European Economic Area

1. Some of our providers are US companies. Even when data is stored in the EU (Frankfurt), the provider may access it from the USA, e.g. for technical support. That is why **we do not claim that all data stays in the EU.** The databases are stored in Frankfurt (EU). The database provider is based in the USA and may have service access to them. This access is safeguarded under the EU-US Data Privacy Framework and standard contractual clauses (SCCs). It is similar with the AI Assistant: the AI model processes data in the EU, but Google may access it from outside the EEA, e.g. for technical support or abuse checks (sections 5 and 11).
2. Transfers are based on the European Commission's adequacy decision for companies certified under the **EU–US Data Privacy Framework** (Article 45 GDPR) or on **standard contractual clauses** adopted by the Commission (Article 46(2)(c) GDPR). The basis for each provider is given in the table in section 11. For Neon and Vercel we carried out a transfer impact assessment. The additional safeguards today are: databases in the Frankfurt region, encryption in transit (TLS) and at rest by the providers, and a separate database, with separate credentials, for sign-in data and account data (the financial database holds no e-mail, name or picture address), as well as encryption of

selected fields in the app (section 16.4). You can obtain a copy of the safeguards by writing to contact@cointrack.pl.

3. When you connect an external AI assistant yourself (Connected AI apps), data goes to its provider **on your instruction**. You decide on that transfer, and the provider is responsible for it under its privacy policy.

13. Profiling and automated decisions

1. CoinTrack automatically calculates budget summaries and the balance at the end of the month, suggests a category (in the expense form - the categories your Family used most in the last 90 days; for a Task - a category based on the words in its title, from a fixed list, without AI; during import - the category remembered for the merchant, and if there is none and you have not turned this option off - with the help of AI, section 8), matches imported operations with your entries and Tasks (without AI, section 8), suggests how much to deposit to a goal in a given month, calculates the emergency fund in months of expenses and shows progress on goals and limits. You can change the suggestions; an entry is saved only once you approve it. This is profiling within the meaning of the GDPR (Article 4(4)), carried out solely to provide the service to you (Article 6(1)(b)).
2. **We do not make decisions about you based solely on automated processing that produce legal effects or similarly significantly affect you** (Article 22 GDPR). We do not assess creditworthiness or create scoring.
3. We do not profile you for marketing purposes based on Budget data.

14. Service messages and marketing

1. **Service messages** (sign-in link, contract confirmation, payment confirmations, notices of a failed payment, reminders of the end of the Plan Period and of the move to the Free Plan, confirmation of a withdrawal or a refund request, notices of the grant, refusal, return and expiry of a referral programme Discount, notices of a Family handover, of its Owner's account deletion with the Family's deletion date and of its takeover, document changes, security alert) are sent by e-mail under the contract, through Resend (section 11), in the language you use the app in. They contain no advertising. A message that could not be sent is tried again over a few days; for that we do not store your e-mail address or name - we read them again from your account data. A retried confirmation of a withdrawal from the contract does not contain the full name or the note from the form, because we do not store them, and a copy of the confirmation to an extra address is not retried. Family messages are the exception: we send them once, and the same information is shown in the app. The Family invitation message (section 7(2)) is sent on the basis of legitimate interest (section 4), in the inviter's language, also to people without an Account. It contains no advertising. We do not retry it automatically: if it cannot be sent, we do not save the invitation. Only the Owner can resend it, and for that we use the encrypted address record, because the invited person may not have an Account.
2. **Marketing** (e.g. news, offers, tips) is sent by e-mail **only if you give a separate consent**. We do not send push notifications. You can withdraw consent with one click ("Unsubscribe" in the e-mail) or in Settings → Privacy. Withdrawal does not affect the lawfulness of earlier sending.

15. Analytics, cookies and offline mode

We enable PostHog analytics (EU Cloud) **only with your consent**, given in the banner or in Settings → Privacy. We do not send amounts, transaction descriptions, shop names, expense categories, receipt content or chat content to analytics. In analytics we identify you only by a pseudonym, never by e-mail or name. Details: Cookie Policy.

Offline mode. We make it available no earlier than on the day this version of the Policy takes effect. You switch offline mode on yourself, separately on each device (Settings → "Offline mode on this device"); it is off by default. Until you switch it on, we do not store the data in point 1 on the device. Once you switch it on:

1. **What we store on your device:** the last fetched pages of the Dashboard and of the current month's Budget (with the Budget data shown on them and the date and time they were fetched) and the app files needed to open them - in the browser cache (Cache Storage); new expenses and income saved without internet (name, amount, date, category, a random entry key) - in the browser's database (IndexedDB); the identifier of your Account (pseudonym) and of the Family this data belongs to, and the fact that offline mode is on on this device - in localStorage. A CoinTrack script running in the browser (a service worker), which we start only once you switch offline mode on, stores and reads them. Details in the Cookie Policy.
2. **Why:** to show you the last data without internet and not to lose an entry you saved without a connection. Once the connection is back, we send the entry with its key, so it is not saved twice. We do not send the data on the device anywhere other than our server, and only what you see or type in anyway stays on the device.
3. **For how long:** an entry - until it is sent (it leaves the device once the server answers); the Dashboard and Budget pages - until the next fetch replaces them, and we delete a copy older than 30 days; everything - at most until you switch offline mode off, sign out, switch the Family or delete your Account on this device. When another person signs in on the device or opens another Family, we first delete the previous one's data. If your session expires without signing out, or you delete your Account on another device, we delete this data the next time CoinTrack is opened on this device, when the app finds that you are not signed in.
4. **How to delete it:** switch offline mode off (Settings → "Offline mode on this device"), sign out or delete the site data of cointrack.pl in your browser settings. Entries still waiting to be sent are then deleted and do not reach the budget.
5. CoinTrack does not encrypt the data on the device (section 16.4 concerns our databases). It is protected by the browser, which keeps each site's data apart, and by your device's screen lock. Do not switch offline mode on on a device that other people use.
6. You switch offline mode on yourself, separately on each device (Settings → "Offline mode on this device"). Storing on and reading from the device are necessary for the feature you switched on to work, so they do not require consent in the cookie banner (Article 399(3)(2) of the Polish Electronic Communications Law). Switching it off deletes the offline mode data from this device. The legal basis for the processing is the contract (Article 6(1)(b) GDPR).

16. Security

1. Connections are encrypted (TLS). Data in databases and backups is encrypted by the infrastructure providers.
2. Account data and Budget data are in separate databases with separate credentials. Test environments use separate databases. The copy of the production database of 14 October 2026 used in them for testing contains only the service owner's own accounts, not customer data. From the launch of paid Plan sales we do not copy production data to test environments.
3. Only the Service Provider has access to the systems, with multi-factor authentication.
4. **The app additionally encrypts selected fields** (the Family name; the names of income, expenses, recurring entries, custom expense categories and goals; the names and descriptions of assets and liabilities; the merchant and description of imported items; the import file column layout; merchants remembered with a category; the content of conversations with the AI Assistant and the record of changes made in the chat (the data before and after the change; we do not store receipt photos); the title and note of a Task and the payee from an import remembered for it; the e-mail address of a person invited to a Family who does not yet have an Account; fields added later - from their introduction) with data keys protected by a master key in Google Cloud KMS in the Frankfurt region (Germany); the master key never leaves KMS.
5. In the event of a personal data breach that may pose a risk to you, we will notify the President of UODO within 72 hours and, if the risk is high, we will also notify you.

17. Your rights

You have the right to:

1. **access** your data and receive a copy (Article 15);
2. **rectification** of data (Article 16) - you can change most of it yourself in Settings;
3. **erasure** of data (Article 17) - among others by deleting your Account;
4. **restriction** of processing (Article 18);
5. **data portability** (Article 20) - you can download a JSON file with the data you gave us (account data, Families with their Budget data, including Tasks and their check-offs, the chat history with the AI Assistant together with the proposal cards - without receipt photos, because we do not store them) yourself in Settings → Privacy → “Download my data”; other data (e.g. billing data and the record of changes made in the chat: the data before and after the change and the history of the proposal status, section 5(4)) we will provide on request sent to contact@cointrack.pl, within one month at the latest, in a commonly used, machine-readable format;
6. **object** to processing based on legitimate interest (Article 21), and to marketing - at any time;
7. **withdraw consent** at any time, without affecting the lawfulness of processing before the withdrawal (Article 7(3));
8. **lodge a complaint with the President of the Personal Data Protection Office** (ul. Stawki 2, 00-193 Warsaw, Poland, https://uodo.gov.pl).

Send requests to contact@cointrack.pl from your Account’s e-mail address or, if you do not have an Account (e.g. you only received a Family invitation), from the address the request concerns. We will

reply within one month (in exceptional cases - up to 3 months, and we will let you know). We may ask you to confirm your identity.

18. Age

CoinTrack is intended for people aged 18 or over - this also applies to Family Members. We do not knowingly collect data of younger people. If we learn that an Account was created by a minor, we will delete it.

19. Changes to this policy

We update the policy when our services, providers or the law change. We inform you about material changes (e.g. a new purpose, a new recipient, a transfer outside the EEA) by e-mail and in the app before they take effect.