



Privacy Policy

VERSION 4.0 · EFFECTIVE FROM 1 SEPTEMBER 2026 · LAST REVIEWED 27 AUGUST 2026

This is the master privacy notice for CashXChain. It describes the personal data we process as a controller in our own right — for identity verification, financial-crime screening, fraud prevention, security, record-keeping and our own legal compliance — and it is our information notice under Articles 13 and 14 of the [General Data Protection Regulation \(GDPR\)](#) ⁷.

It is a notice, not a contract term. It informs you; it does not create obligations between us and does not vary the [Terms of Service](#). Where we process personal data on a customer's instructions, our contractual obligations are in the [Data Processing Addendum pursuant to Article 28 GDPR](#) (the "DPA").

1. Who is responsible

1.1 The controller is CashXChain UG (haftungsbeschränkt), Georg-Bichler-Str. 9, 83620 Feldkirchen-Westerham, Germany, registered under HRB 34664 at Amtsgericht Traunstein.

1.2 You can reach us on any data protection matter at privacy@cashxchain.com. That address is our contact point for data subject requests and reaches the people who can answer them.

1.3 CashXChain Inc. (Delaware, USA) is the parent holding company. It holds the group's intellectual property and does not process personal data of platform users in the ordinary course. Where that changes, this notice will say so.

2. Who this notice is for

2.1 This notice applies to the representatives, authorised users, directors and beneficial owners of our business customers; to people who contact us, use our websites or subscribe to our updates; to the payees and counterparties of transfers processed through the platform; and to visitors to our public sites.

2.2 Job applicants are covered by a separate document, the [Recruitment Privacy Notice](#), not by this one.

2.3 Our services are for businesses. We do not process the personal data of anyone under the age of 13, and the platform is not directed at consumers. Where we learn that we hold such data, we delete it.

3. Our role, and our Partners' roles

3.1 For the processing described in this notice we act as an independent controller. We determine the purposes and the means ourselves, we are accountable for it ourselves, and we do not act on our customers' instructions when we do it. This covers identity and business verification, financial-crime and sanctions screening, fraud and abuse prevention, platform security, statutory record-keeping, our own accounting and tax obligations, and the defence of legal claims.

3.2 We act as a processor only where we handle personal data purely on a customer's documented instructions in delivering the service. That processing is governed by the [DPA](#), and the sub-processors involved are named on the [Sub-processor List](#).

3.3 A customer cannot instruct us out of the processing in clause 3.1. Where a customer's instruction would conflict with an obligation we owe in our own right, our own obligation prevails.

3.4 Our Partners — the licensed institutions that perform the regulated payment, exchange, custody and settlement steps — are controllers for the personal data they process under their own licences. They are not our processors, and we are not theirs. Their own privacy notices apply to that processing. The current Partners are named on [Regulatory Status & Partner Disclosure](#).

3.5 That control is not of the same kind with every Partner. With most, the Partner determines the purposes and means entirely by itself and answers for that processing alone; Stripe is in that position. With some, we and the Partner determine the purposes and means of certain processing together and are joint controllers for it under Article 26 [GDPR](#) ⁷; that is the position under our agreement with Sokin for the onboarding, account and instruction data we pass to it. Where we are joint controllers you may exercise your rights against either of us, and Article 82 [GDPR](#) ⁷ makes each of us liable for the whole of the damage caused by processing that infringes the Regulation, so you may claim the full amount from either. An arrangement under Article 26 [GDPR](#) ⁷ allocates the responsibilities between the joint controllers; its essence is published on our [Sub-processor List](#) once it is in place.

4. What we process and where it comes from

4.1 From you, or from the business you represent. Company name, legal form, registration number, registered and trading addresses, business activity and the countries you transact with. Name, role, business email address, business telephone number, date of birth, nationality and identity document details for authorised users, directors and beneficial owners. Ownership and control structure, and source-of-funds information.

4.2 From your use of the platform. Account and sub-account records, authentication events, session and device information, IP address, API keys and their use, support correspondence, and the configuration choices you make.

4.3 Transaction data. Amounts, currencies, timestamps, references, originator and beneficiary identifiers, the settlement route taken, and the outcome of any screening applied.

4.4 From third parties. Verification results and risk indicators from our Partners and from identity, sanctions, politically-exposed-person and adverse-media screening providers. Company information from commercial registers and other public sources. Where you sign in with Google, Apple, Microsoft, GitHub or LinkedIn, the basic account information you authorise that provider to release.

4.5 About people who are not our customers. Where your business pays a payee, we process the payee's name, account identifier and the payment reference, together with any information required to accompany the transfer.

4.6 We do not process special categories of personal data under Article 9 [GDPR](#) ⁷ as a routine matter. Where screening for politically exposed persons or adverse media surfaces such information incidentally, we process it only so far as Article 9(2)(g) [GDPR](#) ⁷ permits, for the substantial public interest in preventing financial crime.

5. Why we process it, and on what legal basis

Purpose	Legal basis
Providing the platform and performing the contract with your business	Art. 6(1)(b) GDPR ↗ — performance of a contract, or steps before entering into one. For your representatives personally, Art. 6(1)(f) GDPR ↗
Verifying business identity, ownership and control before and during the relationship	Art. 6(1)(c) GDPR ↗ where a legal obligation applies to us; otherwise Art. 6(1)(f) GDPR ↗
Financial-crime, sanctions and adverse-media screening	Art. 6(1)(c) GDPR ↗ for obligations that apply to us directly, and Art. 6(1)(f) GDPR ↗ for the checks we run beyond them. Art. 9(2)(g) GDPR ↗ where special categories are unavoidably involved
Fraud prevention, abuse detection and platform security	Art. 6(1)(f) GDPR ↗
Voluntary reports to competent authorities where we identify indicators of serious crime	Art. 6(1)(f) GDPR ↗ , and Art. 6(1)(c) GDPR ↗ where a report is required
Accounting, tax and commercial record-keeping	Art. 6(1)(c) GDPR ↗
Establishing, exercising and defending legal claims	Art. 6(1)(f) GDPR ↗
Service messages about the platform, incidents and changes to these documents	Art. 6(1)(b) and Art. 6(1)(f) GDPR ↗
Marketing emails you asked to receive	Art. 6(1)(a) GDPR ↗ — consent, withdrawable at any time
Non-essential cookies and similar technologies	Art. 6(1)(a) GDPR ↗ and § 25(1) TDDDG ↗ — consent

5.1 Our legitimate interests. Where we rely on Article 6(1)(f) [GDPR ↗](#), the interests are: operating a payment platform that is not used for crime, protecting our customers and our infrastructure from fraud and abuse, keeping our relationships with regulated Partners, and defending ourselves against claims. We weighed those against the interests and rights of the people concerned and concluded the processing is proportionate: it uses business rather than private contact data, it is limited to what the purpose requires, and it is what a business dealing with a payments provider would expect. You may object under Article 21 [GDPR ↗](#), and we tell you how in clause 12.

5.2 The anti-money-laundering, sanctions and transfer-information obligations that attach to the regulated steps are met by our licensed Partners under their own regulatory perimeter. Where information must accompany a transfer under [Regulation \(EU\) 2023/1113 ↗](#), it is used only to prevent, detect and investigate money laundering and terrorist financing, and for no other purpose. Our own position is set out on the [Public AML Statement](#).

6. Who receives the data

6.1 Processors acting for us. Hosting, infrastructure, identity verification, screening, support tooling and email delivery providers, each under a contract meeting Article 28 [GDPR ↗](#). They are named on the [Sub-processor List](#).

6.2 Partners as controllers. The licensed institutions that perform the regulated steps receive the data they need for those steps and are responsible for it in their own right, including any reporting to a financial intelligence unit. With most Partners that responsibility is theirs alone; with a Partner we are joint controllers with, it is shared, on the basis set out in clause 3.5.

6.3 Authorities. Competent supervisory, tax, law-enforcement and judicial authorities, where the law requires it or where we make a voluntary report of suspected serious crime. Where the law prohibits us from telling you that a report has been made, we will not tell you.

6.4 Professional advisers and, in a corporate transaction, a prospective acquirer under a duty of confidence.

6.5 We do not sell personal data, do not share it with advertisers, and run no cross-site tracking or ad-tech on any CashXChain property. See the [Cookie Policy](#).

7. Transfers outside the European Economic Area

7.1 Where we or a processor process personal data outside the EEA, we rely on an adequacy decision of the European Commission where one covers the destination, and otherwise on the European Commission's Standard Contractual Clauses together with a transfer impact assessment and any supplementary technical and organisational measures the assessment shows are needed.

7.2 Destinations, recipients and the safeguard relied on for each are listed on the [Sub-processor List](#). You can ask us for a copy of the safeguards at privacy@cashxchain.com.

8. The blockchain

8.1 Settlement uses stablecoins on public blockchain networks. Only technical transaction data and wallet addresses reach a blockchain — not names, not contact details, not identity documents.

8.2 Entries on a public blockchain cannot be altered or deleted by us or by anyone else. Your right to erasure therefore cannot extend to anything recorded on a blockchain. It applies in full to the data we hold off the blockchain, and we will act on it there.

8.3 A wallet address may in principle be linkable to a person by someone who holds other information. We do not publish the link, and we treat the mapping between an address and an identified customer as personal data subject to this notice.

9. Payees and others who are not our customers

9.1 Where your business pays a payee, we process the payee's data under Article 6(1)(b) [GDPR ↗](#) as necessary to perform the payment your business instructed, under Article 6(1)(c) [GDPR ↗](#) for the information that must accompany a transfer, and under Article 6(1)(f) [GDPR ↗](#) for screening and fraud prevention.

9.2 We did not obtain that data from the payee, so Article 14 [GDPR ↗](#) applies. Contacting every payee of every transfer individually would involve disproportionate effort within the meaning of Article 14(5)(b) [GDPR ↗](#). We therefore make this notice publicly available at legal.cashxchain.com/privacy instead, and our customers are required to point their payees to it.

9.3 A payee has the same rights as anyone else under clause 12 and can exercise them at privacy@cashxchain.com.

10. How long we keep it

Data	Retention
Accounting and commercial records	Ten years, per § 147 AO ↗ and § 257 HGB ↗
Verification and screening records we hold in our own right	Five years after the end of the business relationship, aligned with the period that applies to our Partners
Transaction records	Ten years, as part of the accounting record
Account, authentication and security logs	Twelve months, longer where needed for a specific investigation
Support correspondence	Three years after the matter is closed
Records relating to a voluntary report to an authority	As long as necessary for that purpose and to establish, exercise or defend legal claims
Marketing consent and its withdrawal	Three years after withdrawal, as evidence that consent was properly obtained

10.1 Where a period above has run but the data is still needed to establish, exercise or defend a legal claim, we restrict the processing rather than delete it, and delete it when the claim is resolved.

10.2 Otherwise we delete or anonymise personal data once the purpose for which we hold it has ended.

11. Automated decision-making and profiling

11.1 Our systems score and flag transactions, accounts and counterparties, and apply rules that can hold, delay or decline an instruction. That is profiling within the meaning of Article 4(4) [GDPR ↗](#).

11.2 As a matter of policy, a decision that produces legal effects concerning you or similarly significantly affects you — restricting or suspending access, closing an account, or refusing the business relationship — is not taken by automated means alone. A person reviews the case before the decision is final.

11.3 Some controls necessarily act before a person can look at them. A sanctions match, for example, blocks an instruction at the moment it is detected. To the extent that such a control falls within Article 22(1) [GDPR ↗](#), it is permitted under Article 22(2)(a) [GDPR ↗](#) because it is necessary for entering into or performing the contract between us, and under Article 22(2)(b) [GDPR ↗](#) because it is authorised by Union and Member State law to which we and our Partners are subject.

11.4 In either case you may obtain human intervention, put your point of view and contest the outcome by writing to privacy@cashxchain.com or compliance@cashxchain.com. We may be unable to give you the reasons where disclosure would breach the law, a regulatory requirement, a confidentiality obligation, or a restriction relating to an ongoing investigation.

11.5 Freezing funds is not something we can do. Funds sit with a licensed Partner, and any freeze is that Partner's decision under its own obligations.

12. Your rights

12.1 Subject to the conditions in the [GDPR ↗](#), you have the right to:

- access your personal data and receive a copy (Art. 15);
- have inaccurate data corrected and incomplete data completed (Art. 16);
- have data erased (Art. 17), except where we must keep it by law or need it for legal claims, and except for anything recorded on a blockchain;
- restrict processing (Art. 18);
- receive data you gave us in a portable form and have it transmitted to another controller where technically feasible (Art. 20);
- object to processing based on legitimate interests, on grounds relating to your particular situation (Art. 21), and to object at any time and without reason to direct marketing; and
- withdraw consent at any time, without affecting the lawfulness of processing before the withdrawal (Art. 7(3)).

12.2 Write to privacy@cashxchain.com. We answer within one month and may extend that by two further months for complex requests, telling you if we do. We may ask for information to confirm your identity, and we use it only for that purpose.

12.3 Exercising these rights is free. We may charge a reasonable fee, or refuse, where a request is manifestly unfounded or excessive, and we will explain why.

13. Complaints and supervisory authority

13.1 You can complain to a supervisory authority under Article 77 [GDPR ↗](#), in the Member State of your habitual residence, your place of work, or the place of the alleged infringement.

13.2 The authority competent for us is the [Bayerisches Landesamt für Datenschutzaufsicht \(BayLDA\) ↗](#), Promenade 18, 91522 Ansbach, Germany.

13.3 We would rather hear from you first, at privacy@cashxchain.com. Complaints about the service itself follow the [Complaints Procedure](#).

14. Data protection officer

14.1 We have not appointed a data protection officer. We assessed the question against Article 37(1) [GDPR ↗](#) and [§ 38\(1\) Bundesdatenschutzgesetz ↗](#): we are not a public authority, our core activity is not regular and systematic monitoring of data subjects on a large scale, we do not process special categories on a large scale, and fewer than twenty people are constantly engaged in the automated processing of personal data.

14.2 We keep this under review and will appoint a data protection officer, and publish the contact details here, if the position changes. In the meantime privacy@cashxchain.com is the contact point for all data protection matters.

14.3 We are established in the European Union, so no representative under Article 27 [GDPR ↗](#) is required.

15. Cookies, security and changes

15.1 Cookies. What we store on your device, why, and how to control it is set out in the [Cookie Policy](#).

15.2 Security. The technical and organisational measures we apply are summarised in the [Security Statement](#). How we handle a personal data breach is set out in the [Incident Notification Policy](#).

15.3 Changes. We publish the current version here and keep earlier versions, with the dates each applied, in the [Versioned Terms Archive & Change Log](#). Where a change materially affects how we process your data, we will tell you before it takes effect.