cXc

A TRADING NAME OF CONXCHANGE PVT LTD

EXTERNAL PRIVACY NOTICE

Privacy Notice

How we collect, use, and protect personal data

v1.0 · Effective [DD Month YYYY] · Classification: Public

Document	Privacy Notice (External)
Version	1.0
Effective Date	[DD Month YYYY]
Last Updated	[DD Month YYYY]
Classification	Public
Owner	Data Protection Lead, cXc
Review Frequency	At least annually, or on material change

1. Introduction

cXc respects your privacy and is committed to protecting personal data in accordance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (Regulation (EU) 2016/679), the UK Data Protection Act 2018, and other relevant privacy laws.

This Privacy Notice explains what personal data we collect, how we use it, when we share it, how long we keep it, and the rights available to you. It also tells you how to contact us about any privacy matter.

This notice applies to personal data collected through the cXc website, platform, APIs, applications, support channels, events, marketing interactions, and other business communications.

It is intended for external audiences — including website visitors, users of our services, client personnel, prospective customers, partners, suppliers, and other individuals whose personal data we may process.

2. About cXc

cXc — a trading name of conXchange Pvt Ltd — provides software-as-a-service and platform-as-a-service technology to the insurance industry. Our customers include insurers, managing general agents (MGAs), brokers, distributors, and other insurance-sector participants.

Our role under data protection law depends on the product, module, and contractual arrangement:

- We act as a controller for personal data relating to our own business operations — including website management, sales and marketing, event registrations, recruitment, supplier management, account administration, security monitoring, and customer relationship management.
- We act as a processor where we process personal data on behalf of a customer controller under a contract — typically for policyholder, claims, quote, and underwriting data flowing through our platform.
- We act as a joint controller for specific products where we and a customer jointly determine the purposes or essential means of processing — for example, certain shared fraud-detection or industry-benchmark services.

Where you interact with an insurer, broker, MGA, or other client through services operated by cXc, that organisation's own privacy notice will usually also apply. You should review the relevant client privacy notice to understand how that organisation uses your personal data.

3. How to Contact Us

If you have questions about this notice or about how we handle personal data, you can contact our Data Protection Lead:

Role	Data Protection Lead
Organisation	cXc — conXchange Pvt Ltd
Email	privacy@cxc.services
Postal address	[Registered office address, conXchange Pvt Ltd]
Website	https://www.cxc.services

We have not appointed a Data Protection Officer under Article 37 UK/EU GDPR because the statutory conditions do not currently apply to our processing. This position is reviewed at least annually. We have appointed an internal Data Protection Lead who is the primary contact for privacy queries and regulator engagement.

> **EU Article 27 Representative**
> [Placeholder — to be finalised.] Where cXc offers services to individuals in the European Union without being established there, Article 27 of the EU GDPR may require us to appoint a representative in the EU. This notice will be updated with those representative details once the position is finalised, or confirmed as not required.

4. Scope of This Notice

This notice applies to personal data collected:

- Through our website and related digital properties.
- Through use of our Services, including platform access, support requests, and API interactions.
- Through sales, onboarding, account management, procurement, and partnership processes.
- Through marketing activities, surveys, events, webinars, newsletters, and community forums.
- Through recruitment and supplier engagement.

This notice does not apply to third-party websites, applications, or services not controlled by cXc, even where we link to them. Those third parties are responsible for their own privacy practices.

Where separate contractual terms, data processing agreements, or client-specific privacy notices apply, those documents supplement this notice. If there is a conflict, the specific contractual terms take precedence for the processing they cover.

5. Definitions

In this notice:

- **Personal data** means information relating to an identified or identifiable natural person.
- **Controller** means the person or organisation that determines the purposes and means of processing personal data.
- **Processor** means the person or organisation that processes personal data on behalf of a controller.
- **Special category data** means personal data requiring extra protection under applicable law, such as health data, genetic data, or biometric data used for identification.
- **Services** means the cXc website, platform, APIs, applications, and related support and business services.

6. Categories of Personal Data We Collect

Depending on the nature of our relationship with you, we may collect and process the following categories of personal data:

Category	Examples
Identity data	Name, username, title, and employer
Contact data	Business email address, postal address, and telephone number
Account and profile data	Login details, account preferences, user roles, and support identifiers
Transaction and service data	Account activity, support tickets, service usage, product interactions, and configuration information
Technical data	IP address, device identifiers, browser type, operating system, session information, and log data
Usage data	Website activity, feature usage, analytics data, crash reports, and performance telemetry
Marketing and communications data	Subscription preferences, event attendance, and communication history
Recruitment data	CVs, work history, references, and application records
Payment and billing data	Billing contact details and limited transaction information (payment card data is handled by our PCI-compliant payment processor; we do not store full card details)
Insurance-platform data (submitted by clients)	Customer identifiers, quote data, policy-related information, claims-related information, risk attributes, communications metadata, and other customer records depending on the configured use case

Children's Data

> We do not knowingly collect personal data directly from children through our website or Services.
>
> Where our insurance-platform customers process personal data relating to minors (for example, a child named as a dependant on a household policy), we process that data only as a processor under instructions from the customer controller. Our customers are responsible for the lawful basis, age-appropriate safeguards, and any parental consents that may be required.

Where special category data (such as health information in a claim) is processed through the Services for a client use case, we do so only where the client has confirmed an appropriate Article 9 condition, the processing is contractually authorised, and suitable technical and organisational measures are in place.

7. How We Collect Personal Data

We collect personal data in the following ways:

- Directly from you, for example when you complete forms, register for services, contact us, attend events, request information, or apply for a role.
- Automatically, through cookies, server logs, analytics tools, telemetry, and similar technologies when you use our website or Services. See Section 11 for cookies.
- From our customers, partners, brokers, insurers, MGAs, distributors, or other organisations using our Services.
- From third parties, such as analytics providers, advertising networks, search information providers, recruitment agencies, public registers, identity providers, and fraud or compliance service providers.

8. Purposes and Legal Bases

We process personal data only where we have a valid legal basis under UK/EU GDPR. The table below summarises our main processing activities and the legal bases we rely on.

Purpose	Typical Legal Basis
Providing and administering the Services, accounts, support, billing, and service communications	Contract performance; legitimate interests
Managing customer, supplier, and partner relationships	Contract performance; legitimate interests
Operating, securing, monitoring, and improving the website, platform, APIs, and infrastructure	Legitimate interests; legal obligation where applicable
Sending service notices, technical alerts, and security communications	Contract performance; legitimate interests
Sending marketing communications	Consent where required; legitimate interests where permitted by law
Running events, surveys, and community features	Consent where required; legitimate interests; contract performance
Recruitment and hiring administration	Legitimate interests; steps prior to entering a contract; legal obligation
Fraud prevention, misuse detection, legal compliance, and investigation of claims or disputes	Legitimate interests; legal obligation
Meeting audit, recordkeeping, tax, accounting, and regulatory obligations	Legal obligation; legitimate interests
Processing personal data within client insurance-product workflows	Processed on behalf of the client controller under contract — legal basis determined by the client

Where we rely on consent, you may withdraw your consent at any time. Withdrawing consent does not affect the lawfulness of any processing carried out before withdrawal.

Where we rely on legitimate interests, those interests typically include running and improving our business, securing our systems, preventing fraud, supporting our customers, and managing our commercial relationships. We have balanced these interests against your rights and freedoms and only rely on them where they are not overridden by those rights. You can request information about the balancing test for any specific processing using the contact details in Section 3.

9. Processing Within Insurance Products

cXc provides technology that may support insurance distribution, quote-and-bind workflows, underwriting support, claims intake, customer communications, document handling, API-based transactions, and related operational processes.

In this context, we process personal data made available by our clients through the Services, including customer, policy, prospect, claimant, broker, or representative data. For this data we generally act as a processor and we process it strictly in line with our client's documented instructions, our contract with the client, and applicable law.

Where you wish to exercise privacy rights in relation to personal data submitted by one of our clients, we may direct your request to the relevant client controller, unless we are legally required or contractually authorised to handle it directly. We will tell you when we do this so you know who to follow up with.

10. Who We Share Personal Data With

We share personal data only where it is necessary and lawful. The recipients are:

- Group entities and affiliates, where relevant to our business operations.
- Cloud hosting, infrastructure, analytics, communications, support, monitoring, and security service providers that help us operate the Services.
- Professional advisers, auditors, insurers, and legal counsel.
- Payment processors and billing support providers.
- Recruitment service providers.
- Regulators, law enforcement, courts, and public authorities where legally required or where we have a lawful basis to cooperate.
- Customers, business partners, and authorised users, where necessary to provide the Services.
- Potential acquirers, investors, or transaction counterparties in connection with a merger, financing, restructuring, or sale of our business — subject to appropriate confidentiality and data-protection safeguards.

Where we act as a processor, we engage sub-processors only under written contracts that impose equivalent data-protection obligations, and only with our customer's prior authorisation as required by the applicable Data Processing Agreement. A current list of our sub-processors is available at [https://www.cxc.services/subprocessors] and we notify our customers in advance of any material change.

> **We do not sell personal data.**
> cXc does not sell personal data to third parties, and does not share personal data with third parties for their own independent marketing purposes without your consent.

11. Cookies and Similar Technologies

We use cookies and similar technologies to operate our website and Services, analyse usage, maintain security, remember your preferences, and support communications and marketing activities where permitted.

Where required by law (including under the UK Privacy and Electronic Communications Regulations and the EU ePrivacy Directive), non-essential cookies are used only with your consent.

Detailed information about the specific cookies we use, and how to manage your preferences, is available in our Cookies Notice at [https://www.cxc.services/cookies], and you can change your preferences at any time through our cookie preference tool.

12. International Transfers

We are based in the United Kingdom. Providing our Services may require personal data to be transferred to or accessed from countries outside the UK or the European Economic Area (EEA).

Typical destinations for transfers include:

- Within the UK and the EEA — for example, for cloud hosting in UK or EU Microsoft Azure regions.
- To countries recognised as providing an adequate level of protection under UK or EU adequacy decisions.
- To the United States and other non-adequate countries — for example, for support from our cloud and software vendors, certain analytics services, or enterprise collaboration tools.

Where we make a restricted transfer — meaning a transfer to a country not covered by an adequacy decision — we use one or more of the following transfer mechanisms, with supplementary measures where our transfer risk assessment indicates they are needed:

- The UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses.
- The EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914).
- Other lawful transfer mechanisms recognised under UK or EU law.

You can request further information about the specific transfer safeguards that apply to your personal data by contacting us using the details in Section 3.

13. How Long We Keep Personal Data

We keep personal data only for as long as we need it for the purposes described in this notice, and to comply with our legal, accounting, tax, audit, contractual, regulatory, and dispute-resolution obligations.

The table below sets out typical retention periods. Specific periods may vary where a legal obligation or customer contract requires otherwise.

Category of Data	Typical Retention Period
Website analytics and cookie data	Up to 26 months from collection, unless a shorter period is set in the cookies notice
Marketing communications — while subscribed	Until you unsubscribe or withdraw consent
Marketing communications — suppression list	Retained on a suppression list after unsubscribe to ensure we do not contact you again
Event and webinar registrations	24 months after the event
Customer account data and support records	Duration of the customer relationship + 7 years (UK limitation and tax/accounting requirements)
Supplier and partner records	Duration of the relationship + 7 years
Recruitment data — unsuccessful applicants	12 months from the decision, unless you consent to us keeping it for longer to consider you for future roles
Recruitment data — successful applicants	Transferred into the employee record and retained per the employee retention schedule
Financial, billing, tax, and accounting records	7 years (UK) / longer where required by local law
Security logs and audit trails	12 months online; up to 7 years archived, consistent with our ISMS

Category of Data	Typical Retention Period
Insurance-platform data (as processor)	Per customer contract and documented instructions — typically aligned with insurance-sector retention rules (commonly 6–7 years post-policy-expiry, longer for some long-tail classes)
Records of privacy-rights requests	3 years from closure of the request, to demonstrate compliance

At the end of the applicable retention period, we delete, anonymise, or otherwise securely dispose of personal data. In some cases it may persist briefly in backup media, where it is isolated from live processing and deleted according to our backup rotation schedule.

14. How We Protect Personal Data

We implement appropriate technical and organisational measures, designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

These measures include, among others:

- Access controls, strong authentication, and least-privilege administration.
- Encryption of personal data in transit and at rest.
- Logging, monitoring, and security analytics.
- Secure development practices, code review, and vulnerability management.
- Backup, resilience, and disaster-recovery controls.
- Documented incident-management procedures and regular testing.
- Contractual confidentiality obligations on staff and suppliers, and training on data-protection responsibilities.
- An information security management system aligned with ISO/IEC 27001:2022.

Access to personal data is limited to personnel, contractors, and service providers who have a legitimate business need and appropriate authority.

We maintain procedures to identify, contain, investigate, and respond to personal data breaches. Where required by law, we notify the relevant supervisory authority within 72 hours of becoming aware of a notifiable breach, and we notify affected individuals and clients where required.

No method of transmission or storage is completely secure, but we take reasonable steps to reduce risk and to continuously improve our security posture.

15. Automated Decision-Making and Profiling

cXc does not make solely automated decisions producing legal or similarly significant effects about individuals for our own business operations, unless we tell you otherwise in a service-specific notice.

Where our Services enable customers to use automation, scoring, or AI-supported workflows — for example, in underwriting, pricing, or claims triage — we generally provide the tooling on behalf of the customer. The customer's own privacy notice and governance arrangements will determine how automated decisions are made, communicated, and reviewed, and will explain how you can exercise your Article 22 rights.

16. Your Rights

Subject to applicable law, you have the following rights in relation to your personal data:

- **Access** — to ask for a copy of the personal data we hold about you.
- **Rectification** — to ask us to correct inaccurate or incomplete personal data.
- **Erasure** — to ask us to delete your personal data in certain circumstances.
- **Restriction** — to ask us to limit how we use your personal data in certain circumstances.
- **Objection** — to object to our processing where we rely on legitimate interests or use your data for direct marketing.
- **Portability** — to receive your personal data in a structured, commonly used, machine-readable format, where the processing is based on consent or contract and carried out by automated means.
- **Withdraw consent** — at any time where our processing is based on consent.
- **Complaint** — to lodge a complaint with a supervisory authority. See Section 17.

To exercise any of these rights, contact us using the details in Section 3. We will respond within one calendar month, although we may extend this by up to two further months for complex or numerous requests, in which case we will let you know why.

These rights are not absolute and may be limited by law. Where we act as a processor for a customer, a rights request relating to that customer's data may be forwarded to the customer controller — we will tell you when this happens.

There is normally no fee for exercising these rights. However, we may charge a reasonable fee, or refuse to act, where a request is manifestly unfounded or excessive.

To help us respond, we may need to verify your identity. We only use the information you provide for identity verification for that purpose.

17. Complaints and Supervisory Authorities

If you are not satisfied with how we handle your personal data, we encourage you to contact us first so we can try to resolve the issue. If you remain unsatisfied, you have the right to lodge a complaint with a supervisory authority.

Location	Authority	Website
United Kingdom	Information Commissioner's Office (ICO)	ico.org.uk
European Union	The supervisory authority in your EU Member State of residence, place of work, or place of the alleged infringement	edpb.europa.eu (list of national authorities)

18. Changes to This Notice

We may update this notice from time to time to reflect changes to our business, technology, services, or legal obligations.

The current version is always available on our website. The "Effective Date" and "Last Updated" dates on the cover of this document indicate when the notice was most recently revised. Where changes are material, we will highlight them and, where appropriate, notify you directly.

We recommend reviewing this notice periodically.

19. Related Documents

This Privacy Notice is supported by, and should be read alongside, the following documents where they apply to you:

- Cookies Notice — details the specific cookies we use and how to manage preferences.
- Data Processing Agreement — for customers using our Services as a controller; sets out our Article 28 processor terms.
- Sub-processor List — the current list of sub-processors we use when acting as a processor.
- Trust information — summary of our security and compliance posture, available on request or via our trust portal.
- Customer and client-specific privacy notices — where you interact with cXc through a client, their notice may also apply.