Privacy Policy

Version	3.0
Owner	Data Protection Officer
Last updated	05.10.2026
Change log	1.0 – First publication 2.0 – Added new data processor and updated Section 6 “Transfers outside the EU/EEA” 3.0 – Added references to ITX Nordic AB as our Swedish subsidiary.
Review cycle	Annual, or upon significant change to operations.

1. About this policy

ITX Norge AS and its subsidiary, ITX Nordic AB (together "ITX", "we") is committed to protecting personal data. This policy explains how we process personal data as a data controller—that is, when we decide why and how we process personal data.

ITX Nordic AB is the controller for personal data about its own customers, prospects, suppliers, partners, and job applicants. ITX Norge AS is the controller for all other processing described in this policy.

Important distinction: When you use the ITX platform as an employee or customer of an ITX customer, ITX processes that data as a data processor on behalf of our customer, who is the controller. That processing is governed by the Data Processing Agreement between ITX and the relevant customer, not by this policy. If you are an end user or customer of a business that uses ITX, please contact that business to exercise your rights.

This policy applies to:

- Visitors to itxuc.com and our other public websites
- Prospective customers and people who contact us
- Contact persons at our customers, suppliers and partners
- Job applicants
- Visitors to our premises
- People who report security vulnerabilities to us

2. Data controller and contact details

Controller	ITX Norge AS	ITX Nordic AB
Organization number	998 024 986	559605-2174
Address	Borgeskogen 4, 3160 Stokke, Norway	Svärdvägen 212, 182 33 Danderyd, Sweden
Email	support@itxuc.com	support@itxuc.com
Telephone	+47 236 80 400	+46 8 557 600 70
Privacy inquiries	dpo@itxuc.com	dpo@itxuc.com

3. What we process, why, and on what legal basis

3.1 Website visitors

Personal data	IP address, browser and device type, operating system, referring URL, pages visited, time and duration of visit, language preference, cookie identifiers.
Purpose	Operating and securing the website; measuring and improving content; marketing
Legal basis	Strictly necessary cookies and server logs: legitimate interest (GDPR Art. 6(1)(f)) in operating a secure and functional website. Analytics and marketing cookies: consent (Art. 6(1)(a)), cf. the Electronic Communications Act § 3-15
Retention	Server logs: 12 months. Cookie lifetimes vary by cookie and are listed in our Cookie Policy

Note: The technologies used to collect this data on your device, and how you control them, are described in our Cookie Policy.

3.2 Inquiries, demo requests and sales dialogue

Personal data	Name, employer, job title, email, telephone number, and the content of your inquiry.
Purpose	Responding to enquiries, arranging demonstrations, preparing offers, and following up potential customer relationships
Legal basis	Steps taken at your request prior to entering into a contract (Art. 6(1)(b)), or legitimate interest in responding to business inquiries (Art. 6(1)(f)).
Retention	24 months from the last contact, unless a customer relationship is established.

3.3 Marketing and newsletter

Personal data	Name, employer, email address, and statistics on whether emails are opened and which links are clicked
Purpose	Sending newsletters and information about our services; measuring the effect of our marketing.
Legal basis	Consent (Art. 6(1)(a)), cf. the Marketing Control Act § 15. For existing customers, we may send information about similar services based on the existing customer relationship, cf. the Marketing Control Act § 15 third paragraph.
Retention	Until you withdraw your consent or unsubscribe. Every message contains an unsubscribe link.

3.4 Contact persons at customers, suppliers and partners

Personal data	Name, employer, job title, work email, work telephone, role in the contractual relationship, correspondence, and — for platform administrators — login identifier and activity logs in administrative interfaces.
Purpose	Administering the contractual relationship, delivering and supporting the service, invoicing, account management, and service notifications.
Legal basis	For the duration of the contractual relationship plus 3 months. Accounting documentation is retained for five years after the end of the financial year in Norway, cf. the Bookkeeping Act § 13, and until the end of the seventh year after the calendar year in which the financial year ended in Sweden, cf. the Swedish Bookkeeping Act (bokföringslagen) ch. 7 § 2.
Retention	For the duration of the contractual relationship plus 3 months. Accounting documentation is retained for five years after the end of the financial year, cf. the Bookkeeping Act § 13.

3.5 Support requests

Personal data	Name, contact details, employer, and any information you include in a support request — including screenshots, log extracts and system data.
Purpose	Investigating and resolving reported issues and improving the service.
Legal basis	Performance of the contract with the customer (Art. 6(1)(b)) and legitimate interest in providing effective support (Art. 6(1)(f)).
Retention	24 months from case closure.

Note: Where a support request contains personal data belonging to a customer's own data subjects, ITX processes that data as a processor under the relevant Data Processing Agreement.

3.6 Job applicants

Personal data	Name, contact details, CV, application letter, education and employment history, references, and any results from interviews or assessments.
Purpose	Assessing applications and administering recruitment processes.
Legal basis	Steps taken at the applicant's request prior to entering into an employment contract (Art. 6(1)(b)) and legitimate interest in a documented recruitment process (Art. 6(1)(f)).
Retention	Deleted 3 months after the position is filled, unless you consent to us retaining your application for future opportunities. Open applications sent to karriere@itx.no are retained for 6 months

3.7 Visitors to our premises

Personal data	Name, employer, host, time of arrival and departure.
Purpose	Physical access control, security, and emergency evacuation
Legal basis	Legitimate interest in securing our premises and information assets (Art. 6(1)(f)).
Retention	3 months.

3.8 Security vulnerability reports

Personal data	Name, contact details, and the content of the report, where provided
Purpose	Receiving, assessing and responding to reported vulnerabilities
Legal basis	Legitimate interest in maintaining the security of our services (Art. 6(1)(f))
Retention	24 months after the case is closed.

Note: Reports may be submitted anonymously. See our Vulnerability Disclosure Policy.

4. Cookies and similar technologies

We use cookies and similar technologies on our websites. Under the Electronic Communications Act § 3-15, we may only store information on, or access information in, your device only where you have given prior consent that meets the requirements of the GDPR. This does not apply to technologies that are strictly necessary to deliver a service you have requested.

Our Cookie Policy sets out which cookies and similar technologies we use, who provides them, what they are used for, and how long they remain on your device. You can change or withdraw your consent at any time via the cookie settings icon in the left footer of every page.

Where cookies result in the processing of personal data about you, that processing is described in section 3.1 above.

5. Who we share personal data with

We do not sell personal data. We disclose personal data to:

- **Data processors** who process personal data on our behalf under a data processing agreement. Where ITX Nordic AB is the controller, ITX Norge AS processes the data in our shared systems as its processor, and the providers of those systems act as sub-processors:

  Consent Management provided by *CookieYes Limited, 3 Warren Yard Warren Park, Wolverton Mill, Milton Keynes, MK12 5NW, United Kingdom.*

  Marketing automation provided by *Make AS, Sandakerveien 116, 6 etg., 0484 Oslo, Norway. NO 993 555 002.*

  Team messaging and collaboration provided by *Slack Technologies Limited, One Park Place, Hatch Street Upper, Dublin 2, Ireland.*
  Our workspace is configured for data storage within the EU/EEA.

  Accounting and ERP (ITX Norge AS) provided by *Tripletex AS, Karenslyst allé 56, 0277 Oslo, Norway. NO 914 286 018.*
  Data is stored within the EU/EEA.

  Accounting and ERP (ITX Nordic AB) provided by *Fortnox AB, Bollgatan 3B, 351 06 Växjö, Sweden. SE 556469-6291.*
  Engaged directly by ITX Nordic AB. Data is stored within the EU/EEA.

  Human resources management provided by *Simployer AS, Kalnesveien 5, 1712 Grålum, Norway. NO 986 419 454.*
  Data is stored within the EU/EEA.

  Cloud productivity and collaboration platform provided *by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland.*
  Our tenant is configured for data storage within the EU/EEA.

  AI assistance provided by *Anthropic PBC, San Francisco, California, USA.* Used to support drafting, summarization, and analysis in our

internal work. Data disclosed to this provider is not used to train its models, and is subject to the safeguards described in section 6.

- **Public authorities**, where we are legally obliged to disclose information.
- **Advisers**, such as auditors and legal counsel, where necessary.

6. Transfers outside the EU/EEA

We seek to keep personal data within the EU/EEA. Where personal data is transferred to, stored in, or accessible from a country outside the EEA, we establish a lawful basis for the transfer under Chapter V of the GDPR before the transfer takes place:

- Adequacy decision (Art. 45) — where the European Commission has decided that the country in question ensures an adequate level of protection.
- Standard Contractual Clauses (Art. 46(2)(c)) — the clauses adopted by the European Commission, supplemented where necessary by additional technical, organizational and contractual measures identified through a documented transfer impact assessment.

Recipient	Country	Transfer basis
CookieYes Limited	United Kingdom	Adequacy decision
Anthropic PBC	United States	Standard Contractual Clauses, with supplementary measures

For transfers to the United States, we have carried out and documented a transfer impact assessment. Alongside the Standard Contractual Clauses, we rely on contractual limits on the purposes for which the recipient may process the data, a contractual exclusion of special categories of personal data, access restrictions and confidentiality obligations applying to the recipient's personnel, the recipient's obligations under the Standard Contractual Clauses in the event of a request for access by a public authority, and our own internal restrictions on what personal data may be submitted to the service.

You may request a copy of the safeguards applied to a transfer by contacting dpo@itxuc.com.

7. Security

We have implemented technical and organizational measures to protect personal data against unauthorized access, alteration, deletion, and loss. These include least-privilege access control, encryption of data in transit, logging and monitoring, secure

development practices, supplier assessments, and regular personnel training. Our information security management system is built on ISO/IEC 27001.

8. Your rights

Where we act as controller, you have the right to:

- **Access** — obtain confirmation of whether we process personal data about you, and a copy of that data.
- **Rectification** — have inaccurate or incomplete data corrected.
- **Erasure** — have data deleted where the conditions are met.
- **Restriction** — request that processing be limited.
- **Object** — object to processing based on legitimate interest, including direct marketing.
- **Data portability** — receive data you have provided in a machine-readable format, where processing is based on consent or contract.
- **Withdraw consent** — at any time, where processing is based on consent. This does not affect the lawfulness of processing carried out before withdrawal.

To exercise your rights, contact us at dpo@itxuc.com. We will respond without undue delay and in any event within one month. We may ask you to verify your identity before we act on a request.

9. Complaints

If you believe we are processing your personal data unlawfully, we would like to hear from you first so we can address it. You also have the right to lodge a complaint with the Norwegian Data Protection Authority:

Norway: Datatilsynet
Postboks 458 Sentrum, 0105 Oslo
postkasse@datatilsynet.no
www.datatilsynet.no

Sweden: Integritetsskyddsmyndigheten (IMY)
Box 8114, 104 20 Stockholm
imy@imy.se
www.imy.se

10. Changes to this policy

We may update this policy as our services and our processing activities change. The current version is always available at itx.no. Where changes are material, we will notify affected individuals directly where practicable.