

Privacy Policy – TFK

TFK Logistics

Göteborg, Sweden

This Privacy Policy explains how TFK Logistics (“we”, “us”) processes personal data in connection with our business activities and our website. Transparency and protection of personal data are important to us, and we process personal data in accordance with the EU General Data Protection Regulation (GDPR).

This policy applies to customers, suppliers, business partners, job applicants, visitors to our website, and other individuals whose personal data we process.

1. Data Controller

TFK Logistics is the data controller for the processing of personal data described in this policy.

Contact details:

Data Protection Officer (DPO) and GDPR responsible: **Thomas Illek**

Email: thomas.illek@tfklogistics.com

Phone: +46 73-521 68 01

All privacy-related questions may be addressed to the contact person above.

2. What personal data do we process and for what purposes?

We only process personal data that is necessary for legitimate business purposes, including:

Customers and suppliers

Names, contact details, contract, order and invoicing information to fulfil agreements and manage business relationships.

Business contacts and communications

Names, email addresses, phone numbers and correspondence used for business communication and cooperation.

Job applicants

Information provided in CVs, applications and references for recruitment and assessment of candidates.

Employees

Personnel, payroll and absence data processed to fulfil employment contracts and comply with labour and tax legislation.

Website use

When you visit our website, technical data such as IP address, browser type, operating system, date and time of access and referring pages may be processed to ensure security, stability and proper functioning of the website.

We avoid processing personal identity numbers and sensitive personal data unless required by law.

3. Legal basis for processing

Personal data is processed on one or more of the following legal bases:

- **Contract** – to enter into or fulfil customer, supplier or employment contracts
- **Legal obligation** – for example accounting, labour law and tax requirements
- **Legitimate interest** – for business communication, administration, IT security and maintaining business relationships
- **Consent** – mainly for recruitment pools for future positions (consent may be withdrawn at any time)

When processing is based on legitimate interest, our interest consists of conducting and developing our business in a secure and efficient manner. We have assessed that this processing does not override the fundamental rights and freedoms of the data subjects.

4. Is providing personal data mandatory?

In some cases, providing personal data is a contractual or legal requirement. If such data is not provided, we may be unable to enter into or fulfil a contract or comply with legal obligations. In other cases, providing personal data is voluntary.

5. How long do we retain personal data?

We retain personal data only for as long as necessary for the relevant purpose:

- **Recruitment:** normally up to 4 weeks after the recruitment process has ended, or up to 12 months where consent has been given
- **Contractual and financial data:** in accordance with accounting legislation (generally 7 years)
- **Employee data:** in accordance with labour law and social security requirements
- **Website technical data:** retained for a limited period necessary for security and operational purposes

Personal data is deleted or anonymised when it is no longer needed.

6. Sharing of personal data and data processors

We only share personal data when necessary, for example with:

- IT and system providers
- Payroll and financial service providers
- Banks, insurance and pension providers
- Authorities where required by law

When external parties process personal data on our behalf, this is governed by data processing agreements or equivalent contractual safeguards in accordance with the GDPR.

7. Transfers to third countries

If personal data is, in exceptional cases, transferred to countries outside the EU/EEA, such transfers take place in accordance with the GDPR, for example through EU Standard Contractual Clauses or other approved safeguards.

8. Security measures

We implement appropriate technical and organisational measures to protect personal data, including:

- Access control and the principle of least privilege
 - Multi-factor authentication (MFA) where appropriate
 - Encryption and regular backups
 - Incident management and information security procedures
-

9. Your rights

Under the GDPR, you have the right to:

- Obtain information about the personal data we process (right of access)
- Request rectification of inaccurate personal data
- Request erasure or restriction of processing
- Object to processing or withdraw consent
- Receive your data in a structured, commonly used format (data portability)

Requests may be made using the contact details above. We normally respond within 30 days.

You also have the right to lodge a complaint with the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten – IMY).
www.imy.se

10. Automated decision-making

We do not use automated decision-making or profiling as defined in Article 22 of the GDPR.

11. Changes to this policy

This Privacy Policy is updated when necessary, for example due to changes in legislation, business operations or IT environments. The latest version is always published on our website.

Last updated: 2026-03-24