

LÄNSIMETRO OY

PRIVACY STATEMENT FOR PROCUREMENTS

Privacy statement

1 Name of data file

Personal data file concerning the implementation of procurements

2 Controller

Länsimetro Oy (2124310-8)

P.O. BOX 20491

02070 ESPOON KAUPUNKI

3 Person responsible for the data file

Mari Mannila, Director of Administration, Länsimetro Oy

mari.mannila@lansimetro.fi, 040 757 2907

4 Contact person for the data file

Mari Mannila, Director of Administration, Länsimetro Oy

mari.mannila@lansimetro.fi, 040 757 2907

5 Personal data processing – purpose, legal basis and storage periods

Personal data is processed so that Länsimetro Oy can implement its planned procurements and procurement-related measures. Personal data processing is necessary for the implementation of procurements.

Personal data is processed in Länsimetro Oy's procurement processes which may relate to, for instance, market surveys and various phases of the procurement procedure, such as procurement planning, tender processing and comparing, and preparing contracts for signing.

The following table lists each processing activity, the personal data related to the activity, the legal basis for the processing and the data storage periods.

| Processing activity | Data processed | Legal basis | Storage period |
|---|---|---|---|
| Implementation of the procurement procedure (negotiations, offers and comparisons) | <p>The following personal data of the tenderer's contact persons is processed:</p> <ul style="list-style-type: none"> - First and last name - Date of birth - Name of the represented organisation (in some cases) - Phone number - Email address - Title/job title | A legitimate interest (GDPR, Article 6(1)(f)) | 10 years from when a contract ends or from the acceptance of a project. |

| Processing activity | Data processed | Legal basis | Storage period |
|--|--|------------------------------------|---|
| Preparation and administration of contracts (incl. confidentiality agreements) | <ul style="list-style-type: none"> - Photo (if attached to a CV, for example) - Information related to professional qualifications: work experience and education - Recordings: the data subject's voice, video of the data subject (if such has been requested) <p>The following personal data of the contact persons named in the provided references is processed:</p> <ul style="list-style-type: none"> - First and last name - Name of the represented reference organisation (in certain cases) - Email address - Phone number - Title/job title - Information about the reference in question | A contract (GDPR, Article 6(1)(b)) | 10 years from when a contract ends or from the acceptance of a project. |
| | <p>The following personal data of the tenderer's contact persons is processed:</p> <ul style="list-style-type: none"> - First and last name - Date of birth - Name of the represented organisation - Phone number - Email address - Title/job title - Photo (if attached to a CV, for example) - Information related to professional qualifications: work experience and education - recordings (if such has been requested) <p>The following personal data of the contact persons named in the provided references is processed:</p> | | |

| Processing activity | Data processed | Legal basis | Storage period |
|---|---|---|--|
| Implementing market dialogue | <ul style="list-style-type: none"> - First and last name - Name of the represented reference organisation (in certain cases) - Email address - Phone number - Title/job title <p>The following personal data of the tenderer's contact persons is processed:</p> <ul style="list-style-type: none"> - First and last name - Name of the represented organisation - Email address - Phone number - Title/job title <p>The following personal data of the contact persons named in the provided references is processed:</p> <ul style="list-style-type: none"> - First and last name - Name of the represented reference organisation (in certain cases) - Email address - Phone number - Title/job title | A legitimate interest (GDPR, Article 6(1)(f)) | Stored for the duration of procurement appeal periods. |
| Assessment of the tenderer's suitability (criminal record extract) | <ul style="list-style-type: none"> - First and last name - Personal identity code | A legal obligation (GDPR, Article 6(1)(c)) | Not stored. The information is checked, but the extract is not stored. |
| Obtaining security clearance (Finnish Security and Intelligence Service, Supo) | <p>The following personal data of the individual subject to a security clearance check is processed:</p> <ul style="list-style-type: none"> - First and last name - Profession - Job title - Personal identity code | Consent (GDPR, Article 6(1)(a)) | 5 years |

| Processing activity | Data processed | Legal basis | Storage period |
|--|--|------------------------------------|--|
| | <ul style="list-style-type: none"> - Result of the security clearance check | | |
| Invoice payments in accordance with contractual obligations | The following personal data of the tenderer's contact persons is processed: <ul style="list-style-type: none"> - First and last name - Name of the represented organisation - Phone number - Email address | A contract (GDPR, Article 6(1)(b)) | 10 years from the end of the last financial period |

6 Sources of personal data

Länsimetro Oy obtains personal data from the parties involved in the various phases of the procurement process, from the offers it receives and from its contractual partners. Länsimetro Oy obtains criminal record extracts from the supplier that wins the competitive tender.

Personal data is also obtained from publicly available registers and services, such as trade registers and Vastuu Group's Reliable Partner report.

7 Personal data recipients or groups of recipients

Personal data is processed by Länsimetro Oy's personnel or possibly by assisting experts who are not employed by Länsimetro Oy.

Personal data may be disclosed only to a requesting authority as required by law, or if consent to disclose the data has been obtained.

8 Transfer of data outside the EU or EEA

As a rule, personal data is not transferred outside the EU or the European Economic Area (EEA). If data is exceptionally transferred outside the EU/EEA, Länsimetro Oy ensures that the transfer takes place on legal grounds and with adequate safeguards. The transfer may be based on an adequacy decision by the European Commission or on Standard Contractual Clauses (SCCs) approved by the Commission, which ensure an adequate level of data protection. Data subjects are separately informed of such transfers and the safeguards used.

9 Data file maintenance systems

Personal data is stored and processed mainly in the systems listed below. The table lists the provider (organisation) of each system, and the system's purpose, geographical location and possible transfer mechanisms.

| Organisation | Description (Purpose) | Location | Transfer mechanism |
|----------------------------------|---|----------|--------------------|
| Cloudia | A tendering system for managing the procurement process | EU/EEA | N/A |
| ContractZen | A contract management system | EU/EEA | N/A |
| Länsimetro Oy's service provider | A secure network drive for file storage | EU/EEA | N/A |
| Microsoft | A SharePoint environment for internal document management | EU/EEA | N/A |
| Procountor | Financial and payroll management | EU/EEA | N/A |
| Sokopro | Project material management | EU/EEA | N/A |

10 Technical and organisational protective measures

Länsimetro Oy is committed to protecting personal data through appropriate technical and organisational measures to prevent unauthorised access, disclosure, loss, or other unauthorised processing.

Technical protective measures

- **Access control:** Access rights to the systems are based on personal, role-based credentials. Access rights are granted only to the extent required to carry out work tasks, and their use is supervised.
- **Encryption:** Personal data is protected by encryption, both in transit (e.g. TLS/SSL) and at rest (e.g. encryption of databases and files).
- **Protection of the information network:** The information network is protected against external threats by firewalls and other technical solutions.
- **Resilience:** We ensure system resilience and regular data backups to safeguard business continuity.
- **Management of log data:** Log data on the use of the systems is collected and used to monitor and resolve possible data security breaches.

Organisational protective measures

- **Personnel training:** Personnel receive regular training in data protection and information security practices and guidelines.
- **Internal guidelines:** Data processing is guided by internal policies, guidelines and processes.
- **Confidentiality obligation:** Personnel who process personal data are committed to the confidentiality obligation.
- **Physical safety:** Physical (hard copy) data is stored in locked premises with restricted access and access control.
- **Agreements:** Data Processing Agreements (DPAs) have been signed with third-party service providers to ensure their compliance with the GDPR.

11 Rights of the data subject

The data subject has numerous rights under the EU General Data Protection Regulation (GDPR) concerning their personal data. A data subject may exercise their rights by contacting the contact person for the data file (section 4).

- **Right of access by the data subject (Article 15):** The data subject has the right to know whether their personal data is being processed and to receive a copy of that data.
- **Right to rectification (Article 16):** If the data subject's data is inaccurate or incomplete, they have the right to request that their data be rectified.
- **Right to erasure ('right to be forgotten', Article 17):** The data subject has the right to request the erasure of their data under certain conditions, such as when the data is no longer necessary for its original purpose or the data subject withdraws their consent. Statutory obligations (such as the Accounting Act) may, however, limit this right.
- **Right to restriction of processing (Article 18):** In certain situations, the data subject may request the restriction of processing, for example, if they contest the accuracy of the personal data.
- **Right to data portability (Article 20):** The data subject has the right to receive the personal data they have provided in a structured and commonly used format and to transmit that data to another controller when the processing is based on consent or a contract.
- **Right to object (Article 21)** A data subject may object to the processing of their personal data on grounds relating to their particular situation, when the processing is based on a legitimate interest.

12 Right to lodge a complaint

The data subject has the right to lodge a complaint with a supervisory authority (in Finland, the Office of the Data Protection Ombudsman), in particular in the Member State of their habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to them infringes the GDPR.

Contact details of the supervisory authority:

Office of the Data Protection Ombudsman
Visiting address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: P.O. Box 800, 00531 Helsinki
Email: tietosuoja@om.fi Tel. +358 (0)29 566 6700

13 Document updates

Last updated: 19.03.2026