

Privacy Statement – Know Your Customer “KYC” Management Tool

1. Introduction

This Privacy Statement describes what personal data Greenstep and its Group companies (collectively “Greenstep”, “we”, or “us”) collect and how we use that data in our Know Your Customer “KYC” tool.

Greenstep companies are subject to European Union (EU), European Economic Area (EEA) and national legislation on the prevention of money laundering and terrorist financing (“AML”). In this context, we collect and process personal data relating to client representatives and ultimate beneficial owners in order to fulfil our legal obligations and ensure compliance with applicable regulatory requirements. The data is gathered via the KYC Management Tool (Verified), provided by Assently Oy.

2. Controller and contact details

The Controller of personal data processed in accordance with this Privacy Statement is:

Greenstep Oy

Business ID: 2306461-3

Address: Keilaranta 5, 02150 Espoo, Finland

Email: compliance@greenstep.com

In addition, companies belonging to the Greenstep Group act as joint controllers where applicable:

- **Greenstep Sverige AB**, business ID 556683-9717, Drottninggatan 26, 602 24 Norrköping
- **Greenstep Norge AS**, business ID 928556530, Bernt Ankers gate 17, 1534 Moss
- **Greenstep Åland Ab**, business ID 3218063-2, Torggatan 10, 22100 Mariehamn, Åland
- **Greenstep OÜ**, business ID 14679001, Sõpruse pst 145 B-korpus, 3rd floor, 13425 Tallinn, Estonia

Greenstep Oy serves as the primary point of contact for exercising data subject rights and managing compliance-related queries.

For KYC-related matters: kyc@greenstep.fi

3. Basis of processing of personal data

Greenstep processes personal data only where there is a lawful basis under applicable data protection legislation. These include:

- **Performance of a contract**
- **Legal obligation**

Greenstep companies (Greenstep Oy, Greenstep Sverige AB, Greenstep Norge AS, Greenstep Åland Ab, and Greenstep OÜ) are legally obliged to collect and process certain personal data under European Union and national legislation on the prevention of money laundering and terrorist financing.

In accordance with these obligations, Greenstep collects information relating to client representatives and ultimate beneficial owners. In addition, we obtain data from public registers and sources such as Company Register and sanction lists provided by Governmental bodies. This information is used for purposes defined in applicable regulations, including the prevention, detection, and investigation of money laundering and terrorist financing.

Purpose of processing	Categories of personal data	Legal basis
Fulfilling AML legislations	• Identification details of the client and relevant individuals; • Information verifying the authority to represent a company; • Basic information about the client, its representatives, responsible persons, and ultimate beneficial owners, including personal identity numbers where required; • Information assessing whether any of the above-mentioned individuals, or persons closely associated	Legal obligation; performance of a contract

	with them, qualify as politically exposed persons (PEPs), including the basis for such classification; and • Information obtained from applicable sanctions registers and screening processes.	
--	---	--

4. Transfer and disclosure of personal data

Greenstep does not transfer personal data outside the EEA unless appropriate safeguards are in place, such as adequacy decisions by the European Commission or other lawful transfer mechanisms.

Personal data may be disclosed:

- where required by law or competent authorities;
- for the provision of services requested by the data subject;
- in connection with events or services involving third parties;
- as otherwise described in this Privacy Statement.

Personal data collected for anti-money laundering purposes is not disclosed to third parties except where required by law or competent authorities.

Certain authorised personnel of Greenstep subcontractors involved in technical data processing may have limited access to such data. All such parties are contractually bound to comply with applicable data protection legislation, including confidentiality and information security obligations.

5. Storage and retention of personal data

Retention periods are defined based on the nature of personal data, legal requirements, and business needs. Data is stored only as long as necessary and is securely deleted or anonymised when no longer required.

Personal data collected for anti-money laundering and counter-terrorist financing purposes is retained in accordance with applicable legislation. Such data is stored in a reliable manner for

a period of five (5) years:

- after the termination of a regular client relationship; or
- after the completion of an occasional transaction.

After this period, the data will be securely deleted or destroyed in accordance with applicable legal requirements.

6. Protection of personal data

Greenstep has implemented appropriate technical and organisational measures to protect personal data against loss, misuse, alteration, and unauthorised access. Only authorised personnel have access to personal data and are bound by confidentiality obligations.

Personal data is stored in appropriately secured information systems located within the EEA or in jurisdictions recognised by the European Commission as providing an adequate level of data protection.

While we use appropriate safeguards, the transmission of data over the internet cannot be fully guaranteed as secure.

7. Rights of data subjects

Data subjects have rights under applicable data protection legislation, including:

- Right of access
- Right to rectification
- Right to object
- Right to data portability
- Right to erasure
- Right to restriction of processing
- Right to withdraw consent

Requests may be submitted to: **compliance@greenstep.com**

Data subjects also have the right to lodge a complaint with a supervisory authority if they believe their personal data is being processed unlawfully.

- **Finland:** Office of the Data Protection Ombudsman (www.tietosuoja.fi)
- **Sweden:** Integritetsskyddsmyndigheten (www.imy.se)
- **Norway:** Datatilsynet (www.datatilsynet.no)
- **Estonia:** Data Protection Inspectorate (www.aki.ee)

8. Questions and complaints

Greenstep may request additional information to verify identity before responding to requests. Certain rights may be subject to legal limitations.

9. Amendments to this Privacy Statement

This Privacy Statement was last updated on **23 June 2026**.

Greenstep reserves the right to amend this Privacy Statement at any time. Updated versions will be published on our website.