

Approved by the Management Board of the Estonian Internet Foundation on 22 May 2026

Annex 4

eeID Privacy Principles for Data Subjects

1. General provisions

1.1 This document explains how the Estonian Internet Foundation (hereinafter also referred to as EIF) processes the personal data of natural persons in the provision of the eeID electronic identification service.

1.2 This document supplements EIF's general principles for the use of personal data and the contractual terms applicable to the use of the Service. More detailed information regarding EIF's general principles for the processing of personal data is available in the document "Principles for the Use of Personal Data" published on EIF's website.

2. Who processes personal data and what personal data are processed?

2.1 Within the scope of the eeID Service, the Estonian Internet Foundation (registry code 90010019, Paldiski mnt 80, Tallinn) acts as the controller to the extent that EIF organises the operation, security and provision of the eeID platform and Service.

2.2 The respective Client is responsible for the processing of personal data carried out within the Client's e-service or information system in accordance with the Client's own terms and privacy principles. The eeID Service enables Clients to add user authentication and identity verification functionalities to their e-services through various identity services and technical solutions. EIF acts primarily as a technical intermediary of the Service.

2.3 The following personal data may be processed when using the eeID Service:

- first and last name of the natural person;
- personal identification code or other identifier describing the person;
- authentication or identity verification data;
- authentication method data;
- IP address and technical log data;
- Client Application data;
- authentication or identity verification result;
- where video identification is used, video or biometric data in accordance with the terms of the respective service provider.

2.4 EIF follows the principle of data minimisation when processing personal data and processes only such data as are necessary for the provision of the Service, ensuring security or compliance with obligations arising from applicable legislation.

3. Purposes of processing

3.1 Personal data are processed primarily for the following purposes:

- identification and verification of the User's identity;
- enabling secure authentication;
- ensuring the functioning and security of the Service;
- prevention of fraud, misuse and identity theft;
- detection and resolution of technical issues;
- compliance with obligations arising from applicable legislation.

4. Legal basis

4.1 EIF processes personal data on the following legal bases:

- performance of a contract;
- legitimate interests;
- compliance with legal obligations.

5. Third-party service providers

5.1 In the provision of the eeID Service, EIF may use third-party authentication and identity verification service providers (including, for example, Smart-ID, Mobile-ID or Veriff services). Such service providers may act as independent controllers and process personal data in accordance with their own terms and conditions. EIF only intermediates the exchange of data necessary for the functioning of the Service.

In limited cases, personal data may be transferred outside the European Economic Area in accordance with applicable data protection legislation.

6. Data retention and security

6.1 EIF retains personal data only for as long as necessary for the provision of the Service, ensuring security or compliance with obligations arising from applicable legislation.

6.2 The validity of an end-user account or user profile created within the EIF Service is linked to the User's most recent authentication. An account or profile may be considered inactive where the User has not used the Service for a period of five (5) years from the last successful authentication. Data related to inactive accounts or profiles shall be retained only to the extent and for the period necessary for ensuring security, backup purposes or compliance with obligations arising from applicable legislation.

6.3 Appropriate technical and organisational security measures are used to protect personal data, including:

- encrypted communication channels;
- access restrictions;
- logging and security monitoring.

7. Rights of the data subject

7.1 The Data Subject has the right to:

- obtain information regarding the processing of their personal data;
- access their personal data;
- request rectification or deletion of personal data;
- restrict the processing of personal data;
- object to the processing of personal data;
- lodge a complaint with the Estonian Data Protection Inspectorate.

7.2 Questions related to the processing of personal data may be addressed:

- to EIF: info@internet.ee;
- or to the respective service provider (Client) whose e-service was used.