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

Annex 2

Data Protection Terms

1. General provisions

1.1 These Data Protection Terms apply to the use of the eeID electronic identification service provided by the Estonian Internet Foundation (hereinafter EIF) in the legal relationship between the Client and EIF and specify the rights and obligations of the Parties in relation to the processing of personal data.

1.2 This document explains which personal data are processed by EIF in the provision of the eeID Service, for which purposes and on which legal bases, and how the roles of the Parties are allocated in the processing of personal data.

1.3 These Data Protection Terms primarily govern the relationship between the Client and EIF and shall be interpreted together with the Agreement, the Service terms and other applicable legislation.

1.4 Information addressed to natural persons regarding the processing of personal data related to the eeID Service is described in a separate document titled "eeID Privacy Principles for Data Subjects" (Annex 4).

2. Personal Data Processed

2.1 Personal data processed within the scope of the Service include:

2.1.1 User identification data

- personal identification code or other identifier;
- registry code or other legal entity identifier;
- first and last name;
- date of birth;
- country;
- authentication certificate data.

2.1.2 Authentication and identity verification data

- date and time;
- Client Application (including the source from which the user was redirected for authentication);
- authentication method, including for example:
    - bank used in the case of bank link authentication;
    - mobile phone number in the case of Mobile-ID;
    - ID-card;
    - Smart-ID;

    - video in the case of video identification;
- authentication or identity verification result.

2.1.3 Contact details (where necessary):

- name, personal identification code, email address and telephone number of the contact person of the integrated Client.

2.2 Disclosure of Authentication Data

2.2.1 Authentication data shall be disclosed to the Client Application integrated with EIF's authentication service.

2.2.2 When disclosing data, the principle of data minimisation shall be applied. Only the minimum data necessary to confirm the authentication event and identify the authenticated person shall be disclosed. For example, in the case of Mobile-ID authentication, the user's mobile phone number shall not be disclosed to the Client Application integrated with EIF's authentication services.

2.2.3 The result of the authentication (successful or unsuccessful login) shall be visible to the User in the browser.

2.2.4 Encrypted communication channels shall be used when communicating with the Client Application.

3. Purposes, Legal Basis and Disclosure of Personal Data

3.1 Personal data are processed for the following purposes:

- identification and verification of the User's identity;
- enabling secure electronic identification;
- ensuring the functioning of the Service;
- prevention, investigation and resolution of fraud, misuse and identity theft;
- detection and resolution of technical failures;
- investigation of security incidents.

3.2 Personal data are processed on the following legal bases:

- performance of a contract (provision of the Service);
- legitimate interests (security, fraud prevention, investigation and resolution, system reliability);
- where necessary, compliance with legal obligations.

3.3 Personal data shall be disclosed to the Client in accordance with the principle of data minimisation. In the provision of the Service, personal data may be disclosed to third-party service providers solely to the extent necessary for the provision of the Service.

4. Third parties

4.1 EIF may use third-party service providers in the provision of the Service, including authentication, identity verification and other technical service providers.

4.2 Depending on the specific service or processing relationship, third-party service providers may act as independent controllers, processors or sub-processors and shall process personal data in accordance with their own terms and applicable legislation.

4.3 EIF:

- provides technical integration and intermediates data exchange;
- does not determine the purposes or essential means of the personal data processing carried out by third-party service providers to the extent such providers act as independent controllers.

4.4 The Client hereby grants EIF a general authorisation to use third-party service providers and sub-processors necessary for the provision of the Service.

4.5 EIF shall ensure that third-party service providers used in the provision of the Service comply with applicable data protection legislation and implement appropriate technical and organisational security measures for the protection of personal data.

4.6 EIF shall have the right to add, replace or change third-party service providers and processors in accordance with the technical, security or business needs of the Service.

4.7 Information regarding the significant third-party service providers used in the provision of the Service is available in the user environment.

4.8 Where a third-party service provider is located outside the European Economic Area or where personal data are transferred outside the European Economic Area, EIF shall ensure that such transfers are carried out in compliance with applicable data protection legislation, including, where necessary, on the basis of the European Commission's Standard Contractual Clauses or another appropriate legal mechanism.

4.9 EIF is responsible for the lawful transfer of personal data within the scope of its Service.

4.10 EIF shall not be liable for decisions, authentication results, biometric assessments, service interruptions, decision-making logic or the lawfulness of personal data processing carried out by third-party service providers to the extent such processing takes place outside the EIF platform or outside systems under EIF's control.

5. Data transfers

5.1. TIn the provision of the Service, personal data may be transferred outside the European Economic Area where necessary for the technical functioning of the Service, ensuring security, provision of authentication or identity verification services or the use of Service-related support services.

5.2 EIF shall ensure that transfers of personal data outside the European Economic Area are carried out in compliance with applicable data protection legislation and only where:

- the European Commission has adopted an adequacy decision with respect to the relevant country;
- the European Commission's approved Standard Contractual Clauses are used; or
- another data transfer mechanism permitted under applicable legislation is used.

5.3 EIF shall implement reasonable technical and organisational measures to ensure the protection of personal data also in the case of cross-border transfers.

5.4 The Client acknowledges and agrees that third-party service providers or sub-processors used in the provision of the Service may process personal data outside the European Economic Area under the conditions set out in this section.

6. PROCESSING OF PERSONAL DATA IN COOPERATION WITH THE CLIENT

6.1. EIF and the Client may act as joint controllers to a limited extent in connection with the technical performance of authentication or identity verification operations solely to the extent strictly necessary for carrying out the technical authentication or identity verification process. Following transmission of the authentication or identity verification result to the Client, the Client shall act as an independent controller.

6.2 Allocation of Responsibilities

EIF is responsible for:

- the technical functioning and security of the Service on its own platform;
- the authentication and identity verification process;
- the processing of personal data on its platform.EIF processes the personal data of the Client's users to the extent necessary for the functioning of the authentication or identity verification method used by the Client and for the provision of the Service.
    -

The Client is responsible for:

- the processing of personal data within its own systems and e-services;
- providing users with clear and understandable information prior to redirecting them to the eeID Service, including where the user is being redirected and for what purposes their personal data are processed;
- ensuring that users are provided with sufficient and understandable information regarding the processing of personal data within the Client's e-service;
- ensuring the exercise of data subject rights within the framework of its e-service.

6.3 A User may exercise their rights by contacting either EIF or the Client.

6.4 EIF does not determine the purposes, legal basis, retention periods or other essential means of personal data processing carried out within the Client's e-service. The Client independently determines when, on which legal basis and within the scope of which functionalities the eeID Service is used.

6.5 Where the Client uses a service involving video identification, biometric comparison or other identity verification functionality involving elevated privacy risks (including, for example, Veriff services), the Client is responsible for ensuring that:

- the data subject is provided, prior to the use of the Service, with clear and understandable information regarding the processing of biometric data, facial images or other data used for identity verification;
- an appropriate legal basis for the processing of personal data exists in accordance with applicable legislation.

6.6 The Client is responsible for assessing whether the use of the eeID Service or authentication or identity verification services used through it within the Client's e-service requires the carrying out of a data protection impact assessment (DPIA) within the meaning of Article 35 of the GDPR. Where a DPIA is required, the Client shall be responsible for carrying it out. EIF shall cooperate with the Client to a reasonable extent and, where necessary, provide information regarding the technical functioning of the Service.

7. Roles of the Parties in the Processing of Personal Data

7.1. The Parties acknowledge and agree that their roles in the processing of personal data may differ depending on the specific processing activity and the Service used.

7.2. EIF acts as an independent controller in relation to:

- the operation of the eeID platform and user environment;
- ensuring the technical functioning, security and logging of the Service;
- the processing of personal data within EIF's systems;
- processing carried out for statistical purposes, security purposes and the prevention, investigation and resolution of misuse related to the use of the Service.

7.3 The Client acts as an independent controller in relation to:

- the operation of its own e-service, information system or Client Application;
- the provision of services to users;
- the processing of users' personal data within the Client's systems;
- processing carried out for purposes determined by the Client.

7.4 The Parties may act as joint controllers within the meaning of Article 26 of the GDPR to a limited extent in connection with the technical performance of authentication or identity verification operations solely to the extent necessary for:

- intermediating the User's authentication or identity verification request;
- transmitting the authentication or identity verification result;
- ensuring the security and reliability of the Service.

7.5 Where third-party identity verification or video identification services (including, for example, Veriff services) are used in the provision of the Service, the respective service

provider may act either as an independent controller or as a processor in accordance with its service terms and the specific processing relationship.

7.6 EIF does not determine the purposes, legal bases or retention periods of personal data processing carried out within the Client's e-service and shall not be responsible for the Client's independent data processing activities outside the EIF platform.

7.7 The Parties shall notify each other without undue delay of any personal data breach or security incident that may affect personal data processed by the other Party or the security of the Service.

8. Security logs

8.1 Authentication operation data together with data identifying the person shall be logged within the Service for the following purposes:

8.1.1 detecting and investigating misuse of the Service, including identity theft and attempted identity theft, as well as cyberattacks;

8.1.2 detecting and resolving technical failures. Technical failures may include hardware failures, software errors, network connection failures and similar issues;

8.1.3 identifying the causes of technical problems reported by owners of e-services integrated with the Service, including institutions and organisations;

8.1.4 handling user requests and notifications regarding possible security issues or technical failures.

8.2 Access to logs shall be strictly limited on a need-to-know basis. Access shall be granted only to system and service administrators directly involved in operating the Service and, where necessary, officials responsible for investigating security incidents.

8.3 The Client is also recommended to log authentication events on the Client Application side. This is necessary for detecting and investigating both technical failures and misuse of the Service.

9. Data Retention and Security

9.1 Personal data shall be retained only for as long as necessary for:

- provision of the Service;
- ensuring security;
- compliance with obligations arising from applicable law.

9.2 The backup process shall be initiated at least once every twenty-four (24) hours. Backup copies of all Service component data (including configuration data, databases and logs) shall be retained according to the following principle: 7 days / 4 weeks / 12 months. Data may be restored based on backups stored for the days of the current week, the end of the weeks of the current month or the end of the previous 12 months.

9.3 The validity of an end-user account created within the EIF Service is linked to the User's most recent authentication. An end-user account shall 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 end-user accounts shall be retained and backed up in accordance with the backup procedures.

9.4 The following measures are used to protect personal data:

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

9.5 Access to personal data shall be granted only to authorised persons.

10. Exercise of Data Subject Rights

10.1. The Parties shall ensure the exercise of data subject rights in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and applicable legislation within their respective areas of responsibility and with regard to personal data processed within their respective systems.

10.2 Each Party shall independently be responsible for:

- the accuracy, lawfulness and security of personal data processed within its systems and services;
- handling data subject requests to the extent such requests concern systems, services or data managed by that Party;
- compliance with obligations arising from the GDPR within its area of responsibility.

10.3 Where a Party receives a request, complaint or other communication from a data subject concerning, in whole or in part, personal data processed by the other Party or matters falling within the other Party's area of responsibility, the receiving Party shall forward the relevant communication to the other Party without undue delay and, where possible, no later than five (5) working days after receipt.

10.4 The Parties shall cooperate reasonably to facilitate the exercise of data subject rights, including by:

- exchanging necessary information;
- providing each other with reasonable assistance;
- coordinating responses to data subjects or supervisory authorities where necessary.

10.5 EIF is responsible solely for personal data processed on the EIF platform and within EIF systems and shall not be responsible for processing operations carried out within the Client's e-services, information systems or other environments managed by the Client.

10.6 EIF has neither the right nor the technical capability to delete, rectify or restrict personal data processed within the Client's systems or e-services.

10.7 The Client is responsible for ensuring that data subjects are provided, prior to the use of the eeID Service, with adequate information regarding the processing of personal data within the Client's e-service, including information regarding:

- the purposes of processing personal data;
- the authentication or identity verification methods used;
- possible disclosure of data to third-party service providers;
- the possibilities for exercising data subject rights.

10.8 These Data Protection Terms shall not restrict the data subject's right to exercise their rights directly against either Party or to lodge a complaint with the competent supervisory authority.

11. Disclosure of Security Logs

Security logs shall be disclosed where required by law (including, for example, to law enforcement authorities in criminal proceedings or to the data subject upon their request).