



Principles of Processing Personal Data

Version 2.0

Effective from 1 March 2018

This document is the official translation of the original document "Isikuandmete töötlemise põhimõtted". In case of conflict between the original document and the translation, the original shall prevail.

Version and Changes		
Date	Version	Changes
1 March 2018	2.0	<ul style="list-style-type: none">• Changed the title of the document• Revised content and structure• Updated the list of collected personal data• Revised conditions for amending the principles• Added document version information
22 December 2011	1.0	First public version (Principles of Client Data Protection)

1. General information

These principles describe how SK ID Solutions AS (hereinafter referred as "SK") as a data controller ensures the protection of personal data in accordance with applicable laws. The aim of these principles is to provide information for the subscribers on the relevant issues related to personal data processing. These principles do not concern the storage and processing of data of legal persons or other institutions. Should you have any questions relating to the processing of personal data we ask you to contact us using the following contacts:

SK ID Solutions AS

Address: Pärnu mnt 141, 11314 Tallinn, Estonia

Phone: 610 1880

E-mail: info@sk.ee

Fax: 610 1881

Registry code: 10747013

2. Definitions and abbreviations

Subsequently, we explain the definitions and abbreviations used in the present principles.

2.1. What are personal data and what is personal data processing?

Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist. Processing of personal data is any act performed with personal data (incl. collection, recording, storage, alteration, granting access to, retrieval and communication, etc.) or several of the operations, regardless of the manner in which the operations are carried out or the means used.

2.2. Who is a third person?

A third person is any person (both legal and natural persons) who is not a contractual client, employee or authorized data processor of SK.

2.3. What is a certificate?

Digital data that facilitate electronic signing and identity verification, in which the public key relates to the natural person who owns the certificate. Certificates that enable either electronic identity verification or electronic signing are related to personal data.

2.4. What is eIDAS Regulation?

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

As a trust services provider, SK is guided by the eIDAS Regulation in its activities and service provision. The regulation is directly applicable in the European Union, containing requirements and conditions for providing different trust services, including specific requirements for



personal data processing.

3. SK's personal data processing principles

Privacy and personal data protection is very important to us, therefore we have adopted necessary organisational, physical and information technology security measures to ensure the integrity, availability and confidentiality of the data.

We have mapped the personal data we need for service provision and specified the purpose, extent and period of time, we need to store such data. We have laid down requirements and instructions for SK's employees and authorised data processors, how to process personal data in a correct way. We grant access to personal data only for trained employees and authorised data processors, that have passed a relevant background check. SK's employees and authorised staff are aware that they have the right to process personal data only to the extent necessary for them to carry out their duties or, as is the case with authorised data processors, fulfil the contractual obligations.

We confirm that the processing of personal data is legitimate, fit for purpose, minimal, safe and transparent. All our activities are guided by applicable EU and Estonian legislation, policies and principles of SK as well as the present principles of processing personal data. The policies and principles of SK are available on SK's website: <https://sk.ee/repositoorium/>.

4. Purposes of processing personal data

SK processes personal data in order to provide quality services and fulfil its contractual obligations. Furthermore, SK processes personal data in order to fulfil its obligations arising from applicable legislation (e.g. data transmission to research institutions) and, if necessary, to protect its rights that have been infringed upon or contested.

5. Lawfulness of personal data processing

SK processes personal data only in a fair and lawful way, either for the performance of contracts or on the basis of consent. SK confirms that it only collects personal data for the purposes which have been clearly established and are legitimate, and limits the collection of personal data to the minimum necessary for meeting the objectives of such processing. SK only stores personal data as long as necessary for fulfilling the purpose for which the personal data was collected. Please note that we are guided by the eIDAS Regulation when storing personal data in relation to the provision of trust services.

6. Personal data collected

We process your personal data that we need for providing the service when issuing ID-card, Mobile-ID or Smart-ID certificates and when you use the certificates issued by SK for the purposes of authentication or electronic signing.

When we issue and/or serve certificate of ID-card, Mobile-ID or Smart-ID, we process the following data:

- 1 Person's given name and surname;
- 2 Personal identification number;
- 3 Document number;
- 4 Validity period for the document;
- 5 Document type;
- 6 Certificate number;
- 7 Existence of Estonian residency or e-residency;
- 8 Data of the customer service centre;
- 9 In case of Mobile-ID certificate, also the SIM card number, telephone number and mobile phone operator;
- 10 When applying for a Smart-ID certificate, also the person's Smart-ID account number, mobile number, mobile phone data: model and operating system version; e-mail address, bank where the certificate is applied for and bank link confirmation. When issuing a Smart-ID we verify the accuracy of data submitted to us, making use of the population register, confirming the status of the applicant for the certificate (alive, deceased, unknown), information on the existence of guardians or the type of custody rights, if necessary.

If you use an ID-card, Mobile-ID or Smart-ID certificate for the purposes of authentication or electronic signing, we process the following data:

- 1 Person's given name and surname;
- 2 Personal identification number;
- 3 IP address of the information system in which certificate validity information was queried;
- 4 Telephone number and language of communication when using a Mobile-ID;
- 5 IP address of network used by the phone, mobile phone data: model and operating system version when using a Smart-ID;
- 6 Additional information added to electronic signatures (role, city/town, county, postal code, resolution);
- 7 Information on the certificate of other persons (given names and surnames, personal identification numbers) who signed the same data file;
- 8 Data relating to the operations made by the person when using the service (suspension of certificates, termination of suspension, revocation of certificates, issuance of PIN envelopes, renewal of certificates, verification of certificate validity information);
- 9 Data on the electronic service environments and volume of services used by the person (e.g. e-service operations).

During validity confirmation of electronic signatures we process the following data:



- 1 Data file to be signed as transmitted to SK by the information system;
- 2 Names and personal identification numbers of the signatories (certificate data);
- 3 Time of signing and additional information (also the role, town/city, county, postal code, resolution);
- 4 E-service provider;
- 5 Validity of signature.

In providing proxy validity information we process, via e-services, the personal data of the certificate owner also for authentication, signing and validation if these certificates have been issued by another provider of certification services.

If you approach SK with a question, we process your personal data to identify the person asking in order to answer the question or to solve the problem.

SK confirms that it will not process sensitive personal data in the meaning of the Personal Data Protection Act.

7. Right to obtain information and complaint submission

You have the right to receive information from SK regarding your personal data and use thereof in accordance with the procedure and extent laid down in applicable legislation. Moreover, you have the right to require that processing of your personal data be terminated, the disclosure of and granting access to the data be terminated and/or the data collected be deleted or closed if such a right arises from applicable legislation. Please note that the specific requirements regarding the storage of data apply to SK as the provider of trust services in accordance with the eIDAS Regulation and the Electronic Identification and Trust Services for Electronic Transactions Act. To obtain information on one's personal data we ask you to send an e-mail to info@sk.ee.

Should you find that your rights regarding the processing of personal data have been infringed, we ask you to send a complaint via e-mail to kaebus@sk.ee, and we will reply to your e-mail within 30 working days. If you find that SK's response to your complaint is not satisfactory, you may, in the event of infringement of your rights, apply to the courts or the Estonian Data Protection Inspectorate.

Furthermore, you have the right to seek compensation for the material damage caused as a result of the infringement of your rights on the basis of the grounds and procedure laid down in the Law of Obligations Act.

8. Use of data via an authorised data processor

SK has the right, under the contract, to authorise another person (i.e. both natural and legal persons) to process personal data. SK as the controller of data provides the authorised processor with necessary instructions for data processing. SK is responsible for the authorised data processor's compliance with the personal data processing requirements. An authorised data processor may process personal data only for attaining the purpose. SK confirms that a contract for protection of confidential information is in place with all authorised data processors. Authorised processors are, for example, SK's partners in issuing and servicing of certificates and solving client issues.

9. Disclosure or communication of personal data to third persons

SK does not disclose or issue personal data to third persons unless:

- 1 Such an obligation arises from applicable legislation or measures adopted thereunder (e.g. transmission to scientific research institutions);
- 2 Such persons are involved in providing the services;
- 3 SK has the right for the purposes of performing a contract or ensuring contract performance to disclose the data to third persons, including credit information and debt collection companies and other persons handling debt claims, also to legal advisers and bailiffs if the person has failed to comply with the contract;
- 4 The person concerned gives his/her written consent to disclose the information to other third persons.

SK confirms that it will only disclose personal data to third persons to the extent necessary for the purposes for which the personal data are processed.

10. Period of storage of personal data

SK processes personal data as long as necessary for fulfilling the purposes for which the personal data was collected or for fulfilling the obligations arising from applicable legislation.

11. Amending the principles of processing personal data

SK has the right to unilaterally alter these principles of processing personal data in accordance with the requirements laid down in applicable legislation. The amendments will be published on SK's website <https://www.sk.ee/>.