Principles of Processing Personal Data (Privacy Policy)

Version 5.0

Effective from: 5 December 2019

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**
5 December 2019	5.0	• Amended the list of personal data processed • Updated the document structure and content • Added information on the processing of minors' personal data • Added information on the processing of special categories of personal data • Added information on automated decisions • Added information on the sources of personal data • Updated the personal data retention period information • Added data protection officer's contact details
10 December 2018	4.0	• Amended the list of personal data processed • Added explanations about the legal bases for processing • Added information about transferring personal data to e-services
25 May 2018	3.0	Updated according to the requirements of General Data Protection Regulation (hereinafter referred as "GDPR"), which came into force on 25 May 2018
1 March 2018	2.0	• 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 of processing personal data 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. The person representing the legal person or other institution is not considered as natural person; it is an authorized representative of the legal person or other institution whose personal data is not covered by GDPR.

Should you have any questions relating to the processing of personal data we ask you to contact us using the following contacts:

Data controller:

SK ID Solutions AS
Address: Pärnu mnt 141, 11314 Tallinn, Estonia
Phone: +372 610 1880
E-mail: info[A]sk.ee
Fax: +372 610 1881
Registry code: 10747013

Data protection officer:
E-mail: dpo[A]sk.ee

2. Definitions

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

2.1. What is GDPR?

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR)

Personal data is processed according to GDPR, however, please note, that as trust service provider, SK is also guided by the special requirements on personal data processing stipulated in eIDAS Regulation.

2.2. 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.

2.3. 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.

2.4. 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.

2.5. What is a data controller?

‘Data controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Within the context of this document, SK is the data controller.

2.6. What is a data processor?

'Data processor' means a natural or legal person, public authority, agency or any other body which has been contractually appointed by SK to process personal data on behalf of the data controller.

2.7. What is a certificate?

Digital data that facilitate electronical 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 electronical signing are related to personal data.

2.8. What is an e-service?

An e-service is an information system, application or e-environment using services provided by SK (Mobile-ID, Smart-ID, ID-card) for authentication of persons or enabling electronic signatures.

2.9. What is a registration authority?

'Registration authority' is an organisation responsible for the identification and authentication of persons. In addition, a registration authority may accept certificate requests, verify them and/or send them to SK.

3. SK's principles on processing personal data

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 authorized data processors, how to process personal data in a correct way. We grant access to personal data only for trained employees and authorized data processors, that have passed a relevant background check. SK´s employees and authorized 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 authorized data processors, fulfil the contractual obligations.

We confirm that the processing of personal data is legitimate, fair, 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/en/repository/.

SK is certified under the standard ISO/IEC 27001: 2013 "Information technology. Security techniques. Information security management systems." This is a standard, that sets requirements for the organization's information security system management processes and for critical information security assets, including technical, physical and organizational security measures to protect personal data.

4. Sources of personal data

SK obtains personal data from the following sources:

- From the person;
- Personal devices (in case of Smart-ID);
- Registries (e.g. population registers);
- E-service providers;
- Registration authorities and e-identification providers (e.g. banks, mobile operators, the Police and Border Guard Board).

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 or law. 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.

6. What personal data and for what purposes we process?

Personal data may only be processed for specific purposes and processing must have a legal basis.

SK processes personal data on three legal bases: processing is necessary for the performance of an agreement, the data subject has given consent or the processing is necessary for fulfillment of an obligation arising from law.

The processing of personal data for performance of an agreement means that we need personal data to provide a high quality service. We have defined what personal data SK needs for the provision of the service and we keep the amount of personal data processed to a minimum.

Based on your consent we process your biometric data (facial image) for automatic biometric identification. If you send us a query that contains your personal data, then by sending a query, you give SK your consent for processing.

Compliance with obligations arising from law is the processing of personal data that we are required to perform as a service provider by law. For example, we process personal data to respond legally justified queries from investigation authorities.

Below we explain the purpose for processing, legal basis and list of personal data for each action that, where personal data is processed.

Action	Purpose for processing	Legal basis	What personal data is processed?
Issuance and/or servicing certificates	Provision of service	Processing is necessary to fulfill the agreement; Biometric personal data is processed based on consent	1. Person's given name and surname; 2. Personal identification number (when applying Smart-ID certificate, also the country that issued the personal identification code); 3. For Estonian national ID-1 format documents**: document number; validity period for the document; document type; e-mail address at eesti.ee; 4. Certificate number; 5. Existence of Estonian residency or e-residency; 6. Data of the customer service centre; 7. 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); 8. A copy of the identity document used for applying the certificate; 9. An application form for applying certificate signed electronically or with hand-written signature; 10. In case of Mobile-ID certificate, also the SIM card number, the confirmation about the receipt of a SIM card signed electronically or with hand-written signature, telephone number and mobile phone operator (e-mail address in case of certificates of Mobile-ID of Lithuania); 11. For Smart-ID certificate applications, additionally the person's date of birth, Smart-ID account number, telephone number, language of communication, device data: model and version of operating system, device name (*friendly name*), IP address and other technical parameters of the device; email address, bank link confirmation. Upon Smart-ID issuance we verify the correctness of data submitted to us against the population register: for Estonia,

			personal ID number, surname, first name, status of certificate applicant (alive, deceased, unknown), for minors additionally data on the existence of legal guardians and custody type, duration and status; for Lithuania, personal ID number, surname, first name, status of person's data, for minors additionally the personal ID numbers and names of father and mother. 12. Additional information for Smart-ID certificate applications using the automatic biometric identification method: person's country of residence, additional data from document used in registration (document type, country of issuance, document number, citizenship, date of birth, sex, document expiry date, person's facial image, technical data required for document authenticity verification), facial image acquired on biometric identification, video recorded on biometric identification, number of failed registration attempts. 13. For issuance of Smart-ID to persons with no personal ID number, additionally: passport or ID-card number and country of issuance of the document.
Certificate issued by SK is used for the purposes of authentication or electronic signing*	Provision of service	Processing is necessary to fulfill the agreement	1. Person's given name and surname; 2. Personal identification number, for non-Baltic citizens passport or ID-card number; 3. IP address of the information system in which certificate validity information was queried; 4. Telephone number and language of communication when using Mobile-ID; 5. When using Smart-ID, network IP address used by the device, device data: model and version of operating system and other information on the technical parameters of the device; status of PIN numbers; 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 file name; 9. Data file, if sent by information system to SK; 10. E-service provider whose service is used; 11. When using Smart-ID and Mobile-ID, the text sent by the e-service to your device.
Validity confirmation of electronic signatures	Provision of service	Processing is necessary to fulfill the agreement	1. The name of signed data file 2. The data file, if transmitted to SK by the information system; 3. Names and personal identification numbers of the signatories (certificate data); 4. Time of signing and additional information (also the role, town/city, county, postal code, resolution); 5. E-service provider; 6. Validity of signature.
Queries containing personal data	Responding to query	Consent	Data which is transmitted to SK
Queries from investigation authority	Responding to query	Law	Data which is demanded by investigation authority

*When we provide proxy validity confirmation service we process, via e-services, the personal data of the certificate owner for authentication, signing and validation if these certificates have been issued by another provider of certification services.

If you use the certificate issued by the SK for authentication or electronic signing in the e-service, we will transfer your personal data to e-service for the purpose of providing the service. We will only transfer your personal information to e-service with your consent, that means, only if you have initiated the authentication and/or electronic signing transaction by entering the corresponding PIN.

** ID-1 format documents are identity documents meeting ISO/IEC 7810 size requirements, such as ID-card, residence card, digital e-resident ID and diplomat's ID.

6.1. Processing of minors' personal data

SK services are available for use by minors. Minors need parental or guardian consent for qualified Smart-ID registration, concluding a Mobile-ID contract and ID-card applications. Consent requesting is built into the Smart-ID application for qualified Smart-ID registration and minors are unable to use the Smart-ID service without such consent. Only persons over 18 in age may use automatic biometric identification for Smart-ID registration.

Minors may apply for non-qualified or limited-rights Smart-ID Basic within the framework of a banking services contract. If a parent or legal guardian has granted such authorisation via a banking services contract, a minor will not need a separate authorisation for a non-qualified Smart-ID application. You can find out more here about qualified and non-qualified Smart-ID.

A parent or legal guardian assumes liability for the consequences of using services provided by SK (Mobile-ID, Smart-ID, ID-card). They must also explain to the minor the terms and conditions of use of certificates and security requirements of service use.

SK processes the same personal data for minors as for adults, as well as information on parental or legal guardian's consent and the link between the child and parent/guardian (see table in Ch. 6).

6.2. Processing of special categories of personal data

Pursuant to the General Data Protection Regulation, special categories of personal data may be processed if there is the person's explicit consent. If you select the automatic biometric identification method of authentication on Smart-ID registration, SK will ask for your consent to process your biometric personal data during the registration process. The biometric data being processed is a facial image extracted from a video you recorded yourself. Facial image processing is necessary for identity verification on Smart-ID account registration. In addition, SK may perform verifications based on your biometric personal data to ensure the security of your electronic identity and test the quality of the technical solution employed.

If you do not wish your biometric data to be processed, you have the option to select another registration method (internet banking or a customer service point, Mobile-ID, ID-card).

7. Automatic decisions

Under the General Data Protection Regulation a person has the right that no decisions solely based on automatic processing would be made about them that have legal or other material consequences to them. Automatic decisions may be made if necessary to execute a contract between a controller and a person, permitted by law or with a person's explicit consent.

SK will only make automatic decisions based on your biometric data (facial image) using a processor for identification if you select automatic biometric identification for Smart-ID account registration method. In this case SK will ask for your relevant consent during the registration process. If you do not consent to your biometric data being processed and such data being used for automatic decision-making for identification purposes, you have the option to select another authentication method for Smart-ID account registration (internet banking or branch office, Mobile-ID, ID-card).

For contract execution SK will also make automatic decisions based on your personal data regarding certificate issuance or refusal to issue based on data obtained from registries. SK will also validate electronic Smart-ID applications through an automatic decision.

8. Right to obtain information and complaint submission

According to GDPR, a person has the right to access his/her personal data, request rectification, erasure, restriction and data portability.

Information about the operations performed by you with ID-card, Digi-ID or Mobile-ID can be obtained via https://minutoimingud.sk.ee/. You can get information about your Smart-ID accounts and Smart-ID actions via https://portal.smart-id.com. In addition, you may submit a corresponding request to SK.

The prerequisite for exercising the rights listed above, is that the person is uniquely identifiable. Therefore, we kindly ask that you submit corresponding request in electronically signed form to following e-mail address info[A]sk.ee. We will respond to the request within 30 days.

We emphasize that the request cannot be met in the following cases:

- the identity of the applicant cannot be identified;
- the applicant is not legally connected with the data;
- this would be contrary to the requirements of special laws;
- this would be in conflict with SK's legal obligations;
- it may harm the rights and freedoms of another person;
- this may hinder the provision of the service or failure to provide the service;
- this may hinder the work of law enforcement agencies;
- it's not technically possible.

If the processing of personal data is based on consent, at any time you can withdraw your consent by submitting an application in electronically signed form to following e-mail address info[A]sk.ee.

Should you find that your rights regarding the processing of personal data have been infringed, we ask you to send an electronically signed complaint via e-mail to dpo[A]sk.ee, and we will reply to your e-mail within 30 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 (www.aki.ee).

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.

9. Use of data via an authorized data processor

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

An e-service that requests your personal data from SK on the basis of authentication or electronic signing initiated by you, is not the authorized processor of SK under the GDPR.

10. Disclosure or communication of personal data to third persons

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

1. Such an obligation arises from applicable legislation or measures adopted there under (e.g. transmission to investigation authority);
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.

SK discloses your valid Estonian certificates related to identity documents (incl Mobile-ID) during their validity period via the LDAP service. Additional information on the LDAP service is available here.

11. Period of storage of personal data

SK processes personal data only as long as necessary for fulfilling the purposes for which the personal data was collected or for fulfilling the obligations arising from applicable legislation. Please note that in order to provide trust services, we are guided by the eIDAS Regulation and Estonian Electronic Identification and Trust Services for Electronic Transactions Act for the storage of personal data. SK is required to retain personal data for at least 10 years after certificate expiry in order to prove, if necessary, any misuse of your identity and the appropriateness of SK operations in providing services. Retention of data and evidence is required under law and verified by independent auditors and supervisory bodies.

12. 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 www.sk.ee/en and will immediately enter into force.