Principles of processing personal data (Privacy Policy)

Version 7.0

Effective from: 10.10.2022

Version and Changes		
Date	**Version**	**Changes**
10 October 2022	7.0	• Updated and re-structured the list of processed personal data • Added legitimate interest as a legal basis for processing and disclosing personal data • Added secondary subscriber authentication providers as source of personal data • Added information about cookies • Improved explanations and wording
28 September 2020	6.0	• Added information about MyID portal • Added information on the geographical area of data processing • Added information on the possibility to lodge a complaint to the Latvian and Lithuanian supervisory authorities. • Updated the Document structure • Updated website addresses and email addresses
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 while offering Smart-ID and Mobile-ID service and certification service for Estonian ID-card, digi-ID, e-resident's digi-ID, residence permit card and diplomatic identity card. The aim of these principles is to provide information for the subscribers on the relevant topics related to personal data processing and to introduce principles that SK follows while processing personal data.

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 kindly 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]skidsolutions.eu
Fax: +372 610 1881
Registry code: 10747013
Data protection officer:
E-mail: dpo[A]skidsolutions.eu

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.

SK is processing personal data according to GDPR and other relevant data protection legislation, however, please note, that as a 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 operation or set of operations performed with personal data (incl. collection, recording, storage, alteration, granting access to, retrieval and communication, etc.), 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 is natural or legal person, public authority, agency or any other body which 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 is 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?

Certificate is digital data that facilitate electronic signing and identity verification and 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.

2.8. 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, secure and transparent. All our activities are guided by applicable EU, Estonian and other relevant 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.

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, e-identification providers and secondary subscriber authentication 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 manner. SK confirms that it processes personal data only for clearly defined and legitimate purposes and limits the processing of personal data to the minimum necessary to fulfil those purposes.

We process personal data on the following legal bases:

- **Contract execution**: The processing of personal data for the execution of a contract means that we need personal data to provide a quality service. We have determined which personal data SK needs to provide services and are keeping the amount of personal data processed to a minimum.
- **Compliance with legal obligations**: Compliance with legal obligations is the processing of personal data that SK is required by law to fulfil as a service provider. For example, we process personal data in response to legally motivated requests from law enforcement agencies.
- **Consent**: In some cases we process personal data based on data subject's consent. We ask consent for example for processing biometric data in the case of using biometric identification method for registering Smart-ID. In addition, we process based on consent personal data in response to requests containing personal data. In this case the consent for the processing of personal data is given by sending the request to SK.
- **Legitimate interest**: In some cases processing of personal data is based on legitimate interest. This means that processing is necessary for SK or some third party for a purpose that prevails data subject's rights. Based on legitimate interest we process for example some device data for security reasons.

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

SK is processing personal data for the following purposes:

- **Issuing and servicing certificates**: SK is issuing Smart-ID, Mobile-ID and certificates for Estonian identity documents like ID-card, digi-ID, e-resident's digi-ID, residence permit card and diplomatic identity card. SK is also taking care of revoking the certificates and in case of identity documents also suspending and terminating the suspension of the certificates.
- **Enabling usage of the certificates**: SK is enabling the usage of Smart-ID, Mobile-ID and Estonian identity documents for authentication and electronic signing.
- **Handling queries requesting personal data**: In case person him-/herself or investigation or other authority requests personal data from SK, we process the requested data to compile the response. The requester must have lawful basis to request the data. The queries are related to issuing and servicing Smart-ID, Mobile-ID and certificates of identity documents and/or the usage of the certificates for authentication and electronic signing.
- **Handling queries containing personal data**: In case person sends to SK any request that is containing his/her personal data, SK is processing the data to handle the query and respond to it.

Further, we will explain in more detail for each activity, what is the purpose of the processing, the legal basis for the processing and which personal data we process.

Purpose for processing	**Legal basis**	**What personal data is or may be processed?**
Issuing and servicing certificates		
Provision of service	Processing is necessary to fulfill the agreement; Biometric data is processed based on consent	• Person's given name(s) and surname(s); • Personal identification number and the country that issued the personal identification code; • Contact data; • Language of communication; • Identity document data and/or a copy of the identity document used for applying the certificates; • An application form for applying certificate signed electronically or with hand-written signature; • Existence of Estonian residency or e-residency; • Registration method (electronic or in customer service point) and/or data of the customer service point; • Device data (only in case of Smart-ID and Mobile-ID electronic registration); • Certificates data; • Data relating to certificate lifecycle and 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); • SIM-card data and mobile operator (only in case of Mobile-ID); • Date of birth and Smart-ID account number (only in case of Smart-ID); • Additional information for Smart-ID certificate applications using the 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), video recorded on biometric identification, number of failed registration attempts, document validity information from PRADO register. • In case of Mobile-ID and Smart-ID we verify against population register the correctness of name, personal identification number, status of the applicant (alive, deceased) and in case of minors information about legal guardians.
Usage of the certificates for authentication or electronic signing		
Provision of service	Processing is necessary to fulfill the agreement	• Person's given name(s) and surname(s); • Personal identification number, for non-Baltic citizens passport or ID-card number; • IP address of the information system in which certificate validity information was queried; • Phone number and language of communication; • Network IP address used by the device, device data, status of PIN codes in case of Smart-ID; • E-service provider whose service is used; • When using Smart-ID and Mobile-ID, the text sent by the e-service to your device.
Queries requesting personal data		
Responding to query	Depending on the query lawful basis can be consent, law or legitimate interest Note, that the requester can be person him-/herself or investigation or other authority who has lawful basis to request the data.	Data which is demanded by the requester.
Queries containing personal data		
Responding to query	Consent	Data which is transmitted to SK in the request.

When authenticating to e-service or signing a document, personal data (e.g. name and personal identification number) is sent to e-service provider for providing the service. This is done only after PIN code is entered. Entering PIN code is considered as a consent for sending the data.

6.1. Processing of minors' personal data

SK services are available for use by minors. Minors need parental or guardian's consent for qualified Smart-ID registration, concluding a Mobile-ID contract and ID-card applications.

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 about qualified and non-qualified Smart-ID from Smart-ID portal.

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 GDPR, special categories of personal data may be processed based on the person's explicit consent. If you select the biometric identification method for 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 of yourself. Facial image processing is necessary to identify you during Smart-ID account registration. In addition, SK may perform follow-up checks based on your biometric data to ensure the security of your electronic identity and test the quality of the technical solution employed.

Biometric data is not processed in case of other Smart-ID registration methods, like bank link or a branch office, Mobile-ID, Smart-ID, ID-card.

7. Geographical area of data processing

As a rule, SK processes your personal data in the European Union or the European Economic Area. In case we involve authorized processors located outside this area, we do so on the basis of an adequacy decision adopted by the European Commission (EC), sign standard contractual clauses with the partner or implement other appropriate safeguards.

8. Automated decisions

Under the GDPR, a person has the right that no decisions solely based on automated processing would be made about them that have legal or similarly significant consequences to them. Automated decisions may be made if it's necessary to execute a contract between a controller and a person, permitted by law or with a person's explicit consent.

SK makes automated decisions based on your biometric data (facial image) using a processor for identification if you use biometric identification method for Smart-ID account registration. In this case SK will ask for your relevant consent during the registration process. Such automated decisions are not done in case of other Smart-ID registration methods, like bank link or a branch office, Mobile-ID, Smart-ID, ID-card.

SK also makes automated decisions regarding certificate issuance or refusal to issue based on data obtained from registries and validates electronic certificate applications through an automated decision.

Additionally, we make automated decisions to prevent and detect fraudulent activities.

9. Data subject's rights

Data subject has the right to access his/her personal data, request rectification, deletion, transmit of data and restriction of processing.

To exercise the rights listed above, you can send electronically signed request to the e-mail address info[A]skidsolutions.eu. We will respond to your 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 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 is not technically possible.

Additionally, you can access your Mobile-ID, Smart-ID, ID-card and digi-ID accounts and their history on the MyID portal. For ID-card, digi-ID and Mobile-ID you can also see the history of all your transactions (authentication and signing) from there. Information about your Smart-ID accounts and transactions performed with Smart-ID can be found on the Smart-ID portal.

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 e-mail address info[A]skidsolutions.eu.

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]skidsolutions.eu. We will reply to your e-mail within 30 days. If you find that SK is not processing your personal data in accordance with the relevant legislation, you may file a complaint to your national data protection authority (e.g Estonian Data Protection Inspectorate, Latvian Data State Inspectorate, Lithuanian State Data Protection Inspectorate).

10. 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 data processing 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.

11. Disclosure or communication of personal data to third parties

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

- Such an obligation arises from applicable legislation or measures adopted there under (e.g. transmission to investigation authority);
- Such parties are involved in providing the services;
- The third party has legitimate interest to request the data from SK;
- SK has the right for the purposes of performing a contract or ensuring contract performance to disclose the data to third parties, including credit information and debt collection companies and other persons handling debt claims, also to legal advisers and bailiffs if the data subject has failed to comply with the contract;
- The data subject gives his/her written consent to disclose the information to other third parties.

SK confirms that it will only disclose personal data to third parties 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 issued until 02.07.2022) during their validity period via the LDAP service. Additional information on the LDAP service is available here.

12. 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 evidence used for identifying you during certificates issuance for at least 10 years after certificate expiry and logs related to the procedures performed during provision of trust services for at least 10 years in order to prove any misuse of your identity and the appropriateness of SK operations in providing services, if necessary. Retention of data and evidence is required under law and verified by independent auditors and supervisory bodies.

13. Cookies

SK uses cookies on its websites. Cookies are used based on websites Cookie Policies that are available on SK's website.

14. 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 and will immediately enter into force.