Principles of Client Data Protection

Definitions
Client – every natural person or legal entity that uses or has expressed their wish to use the services provided by SK.
SK – state-accredited provider of certification and timestamp services and validity confirmation services, the company that processes Client Data.
Data Protection Inspectorate – the authority that supervises personal data protection.
Client Data – any information about the client that is known to SK (e.g. the client's name, personal identification code, etc.).
Personal Data – any data about a natural person who has been or will be identified irrespective of the shape or form of such data.
Client Data Processing – any operation and several operations carried out with Client Data (incl. Client Data collection, saving, storage and amendment, granting access, making queries, use, forwarding, etc.), irrespective of the manner in which the operations are carried out or the tools used for this purpose.
Principles of Client Data Protection – the document that regulates the basics and the terms and conditions of Client Data Processing in SK.
Service – the certification, time stamp and validity service provided by SK or the Client on the basis of legislation and/or policies.
Third Party – any person (both a natural person or a legal entity, a branch of a foreign company, or a state or local government agency) that is not a Client, SK, an employee of SK or an authorised data processor.
Authorised Processor – the person who processes Client Data on behalf of SK (on the basis of a subcontract).
Certificate – digital data that enable digital signature and digital identification. The certificate that enabled digital identification and digital signature are linked to the client's personal data and can be publicly checked via the personal identification code.

1. Purposes of Client Data Processing

1.1. SK processes Client Data in order to provide services to clients (for the issue and servicing of certificates, provision of the validity confirmation service, etc.), perform its obligations that arise from legislation (i.e. forwarding data to investigating authorities) and, if necessary, to protect its infringed or contested rights.

2. Lawfulness of Client Data Processing

2.1. SK considers client data protection extremely important and guarantees that data are collected and processed pursuant to the laws of Estonia and the generally accepted international principles. SK proceeds in all of its activities from the laws of Estonia, EU standards, the certification and time stamp service principles and policies of SK, and the following Principles of Client Data Protection.

3. Client's Consent to Data Processing

3.1. The Client grants SK their consent to process the Client's data in accordance with these Principles of Client Processing and service provision policies by submitting a written application for use of the Service to SK (either directly or via a contract partner).

4. Composition of Client Data

4.1. The Client processes the following personal data of the Client in order to provide the service:
4.1.1. the first name and surname of the Client;
4.1.2. the personal identification code of the Client, or their date of birth if they have no personal identification code;
4.1.3. the contact details of the Client;
4.1.4. data regarding the identification of the Client (copy of identity document);
4.1.5. data of the certificate issued to the Client;
4.1.6. number and expiry date of the Client's document linked to the certificates issued by SK and the number of the SIM card that the certificates issued by SK are tied to; and
4.1.7. data of the operations carried out by the client during the use of the Service (suspension

of certificates, termination of suspension, annulment, issue of PIN envelopes, renewal of certificates, creation of digital signatures, identification with a certificate), which are primarily required to verify the validity of the certificate and the signature.
4.2. SK does not process private and sensitive personal data for the purposes of the Personal Data Protection Act of Estonia.

5. Client Data Processing for the Purpose of Providing the Service

5.1. The Client is aware that their name and personal identification code are processed and disclosed in the database of valid certificates (pursuant to subsection 94 (6) of the Identity Documents Act). Expired, suspended or annulled certificates are not disclosed in the database of valid certificates.
5.2. The Client is aware and agrees that their certificate, which contains their name and personal identification code, are forwarded to the person who identifies them when certificates are used for digital identification.
5.3. The Client is aware and agrees that their certificate, which contains their name and personal identification code, is added to the digitally signed document when certificates are used for digital signature. SK preserves the digital signature given by the client and the hash of the signed document (the so-called 'digital fingerprint') in order to prove, when necessary, that the digital signature was given at a certain moment in time. Everyone has access to check the digital signature. SK or other persons cannot obtain information about the content of the signed document.

6. Disclosure or Forwarding of Client Data to Third Parties in Other Cases

6.1. SK discloses or forwards the Client Data:
6.1.1. if such an obligation arises from law or any legislation established on the basis thereof (e.g. to investigating authorities);
6.1.2. to persons related to the performance of the contract entered into with the Client or the provision of the Service to be provided;
6.1.3. if the Client is in breach of Contract SK has the right to disclose the data to Third Parties, including credit rating companies (e.g. AS Krediidiinfo), debt collection companies and other persons who deal with debt claims, and to lawyers and bailiffs, in order to perform or guarantee the performance of the contract. When data are disclosed to a credit rating company, the relevant information becomes known to all of the persons who use the database; and
6.1.4. to other third parties with the written consent of the Client.
6.2. SK discloses Client Data to Third Parties only to the extent that is required for the achievement of the purposes of Client Data Processing.

7. Security of Client Data Processing

7.1. SK protects Client Data with strict security and confidentiality rules, and has implemented organisational, physical and technical security measures for the protection of Client Data.
7.2. In Client Data Processing SK does the least that it needs to achieve the purposes of Client Data Processing.
7.3. SK only allows employees who are fully trained and have passed background checks to access Client Data. An employee has the right to process Client Data only to the extent required for the performance of their duties.

8. Changing and Termination of Processing of Client Data

8.1. The Client must immediately inform SK of any changes in their data and circumstances in comparison to the data specified in the documents submitted to SK. SK has the right to demand the document that proves the changes and the Client must submit such a document.
8.2. The Client has the right to view their Client Data. The Client must immediately inform SK if the Client Data are incorrect and submit the correct data required for the provision of the service.
8.3. SK processes Client Data for as long as necessary for the achievement of the purposes of Client Data Processing or the performance of an obligation arising from legislation.

9. Protection of the Rights of the Client

9.1. The Client has the right to:
9.1.1. obtain information about their data and the processing of such data from SK pursuant to

the procedure and to the extent provided for by law;
9.1.2. demand termination of processing and disclosure of their data, termination of allowing access to their data and/or deletion or closure of collected data if such a right arises from the Personal Data Protection Act or any other legislation;
9.1.3. in the event of a breach of their rights in data processing, to demand that the person who caused such a breach terminate such activities; and
9.1.4. turn to the Data Protection Inspectorate or a court at any time in the event of a breach of their rights.

10. Contact Details of SK

10.1. The Client has the right to contact SK using the following contact details if they have any questions about Client Data Processing or in order to file complaints:
10.2.
SK ID Solutions AS
Registry code: 10747013
Address: Pärnu mnt 141, 11314 Tallinn (Delta Plaza House, Floor VI)
Telephone: 610 1880
Fax: 610 1881

11. Amendment of the Principles of Data Protection

11.1. SK has the right to amend the Principles of Client Data Protection unilaterally whilst adhering to the requirements stipulated in the Personal Data Protection Act or other legislation.
11.2. SK informs the Client of any amendments made to the Principles of Client Data Protection on the internet website or in any other manner (e.g. in mass media) at least 1 (one) month before the amendment enters into force.