Data Protection Terms for the ID Software of the Information System Authority

Approved on 26.02.2021

In this document, we explain what personal data is processed by the Information System Authority's (hereinafter RIA) ID software and for what purpose, including to which third party service providers, for what purpose, and what types of data is forwarded.

1. These data protection terms apply to:
   1.1. the DigiDoc4 client;
   1.2. RIA's DigiDoc mobile apps (iOS and Android);
   1.3. RIA's Digital Signature Validation Service (SiVa).

2. The data subject (hereinafter user) is a natural person who uses the ID software.

3. COMPOSITION OF PROCESSED DATA

3.1. The DigiDoc4 client, the RIA DigiDoc mobile application, and the automatic software update control application regularly contact the Information System Authority's server to check for available software and configuration updates. The application transmits to the server:
   3.1.1. the software version number;
   3.1.2. the computer's and phone's operating system name and version number;
   3.1.3. the computer's or phone's language settings:
   3.1.4. the card reader's and card reader driver's information, if connected;
   3.1.5. the user's IP address.

3.2. Upon **signing** with the DigiDoc4 client, the following data will be transmitted to the **validity confirmation service** of SK ID Solutions AS:
   3.2.1. the DigiDoc4 client software version number;
   3.2.2. the DigiDoc library version number;
   3.2.3. the computer's operating system name and version number;
   3.2.4. the format of the envelope (i.e. container) to be signed;
   3.2.5. the serial number of the user certificate;
   3.2.6. the user's IP address.

3.3. Upon **signing** with the DigiDoc4 client, the following data will be transmitted to the **timestamping service** of SK ID Solutions AS:
   3.3.1. the DigiDoc4 client software version number;
   3.3.2. the DigiDoc library version number;
   3.3.3. the computer's operating system name and version number;
   3.3.4. the signature hash (i.e. signature message digest);
   3.3.5. the user's IP address.

3.4. Upon **signing with Mobile-ID** via the DigiDoc4 client, the following data will be transmitted to the **MID REST API web service** of SK ID Solutions AS:
   3.4.1. the DigiDoc4 client software version number;
   3.4.2. the computer's operating system name and version number;
   3.4.3. the user's personal identification code;
   3.4.4. the user's phone number;
   3.4.5. the user's IP address.

3.5. Upon **signing with Smart-ID** via the DigiDoc4 client, the following data will be forwarded to the **Smart-ID service** of SK ID Solutions AS:
   3.5.1. the DigiDoc4 client software version number;

3.5.2. the computer's operating system name and version number;
3.5.3. the user's personal identification code;
3.5.4. the user's IP address.

3.6. Upon validation of digitally signed PDF documents via the DigiDoc4 client, the following data will be transmitted to the Digital Signature Validation Service SiVa of the Information System Authority:
3.6.1. the DigiDoc4 client software version number;
3.6.2. the computer's operating system name and version number;
3.6.3. the user's IP address;
3.6.4. the signed document, including
3.6.4.1. the whole document;
3.6.4.2. the signer's certificate information.

3.7. Upon validation of digitally signed DDOC documents via the DigiDoc4, the following data will be transmitted to the Digital Signature Validation Service SiVa of the Information System Authority:
3.7.1. the DigiDoc4 client software version number;
3.7.2. the computer's operating system name and version number;
3.7.3. the user's IP address;
3.7.4. the signed document, including
3.7.4.1. the title of the envelope (i.e. container) to be signed;
3.7.4.2. the whole document;
3.7.4.3. the signer's certificate information.

3.8. Upon launching the DigiDoc4 client, the following will be transmitted for **loading the Estonian trust list to the trust list holder**, which is the Estonian Information System Authority (sr.riik.ee):
3.8.1. the DigiDoc4 client software version number;
3.8.2. the computer's operating system name and version number;
3.8.3. the user's IP address.

3.9. Upon **uploading a document photo and setting the eesti.ee e-mail address** via the DigiDoc4 client, the following data will be transmitted to the Information System Authority:
3.9.1. the DigiDoc4 client software version number;
3.9.2. the computer's operating system name and version number;
3.9.3. the user's authentication certificate;
3.9.4. the user's IP address.

3.10. Upon **signing** with the RIA DigiDoc mobile application, the following data will be transmitted to the **validation service** of SK ID Solutions AS:
3.10.1. RIA DigiDoc mobile application version number;
3.10.2. the DigiDoc library version number;
3.10.3. the phone's operating system name and version number;
3.10.4. the format of the envelope (i.e. container) to be signed;
3.10.5. the serial number of the user certificate;
3.10.6. the user's IP address.

3.11. Upon **signing** with the RIA DigiDoc mobile application, the following data will be transmitted to the **timestamping service** of SK ID Solutions AS:
3.11.1. RIA DigiDoc mobile application version number;
3.11.2. the DigiDoc library version number;
3.11.3. the phone's operating system name and version number;
3.11.4. the signature hash (i.e. signature message digest);
3.11.5. the user's IP address.

3.12. Upon **signing with Mobile-ID** via the RIA DigiDoc mobile application, the following data will be transmitted to the **MID REST API web service** of SK ID Solutions AS:
- 3.12.1. RIA DigiDoc mobile application version number;
- 3.12.2. the phone's operating system name and version number;
- 3.12.3. the user's personal identification code;
- 3.12.4. the user's phone number;
- 3.12.5. the user's IP address.

3.13. Upon **signing with Smart-ID** via the RIA DigiDoc mobile application, the following data will be transmitted to the **Smart-ID service** of SK ID Solutions AS:
- 3.13.1. RIA DigiDoc mobile application version number;
- 3.13.2. the phone's operating system name and version number;
- 3.13.3. the user's personal identification code;
- 3.13.4. the user's IP address.

3.14. Upon validating the digital signatures of signed PDF documents via the RIA DigiDoc mobile application, the following data is transmitted to the digital signature validation service SiVa of the Information System Authority:
- 3.14.1. RIA DigiDoc mobile application version number;
- 3.14.2. the phone's operating system name and version number;
- 3.14.3. the user's IP address;
- 3.14.4. the signed document, including
  - 3.14.4.1. the whole document;
  - 3.14.4.2. the signer's certificate information.

3.15. Upon validating the digital signatures of signed DDOC documents via the RIA DigiDoc mobile application, the following data is transmitted to the digital signature validation service SiVa of the Information System Authority:
- 3.15.1. RIA DigiDoc mobile application version number;
- 3.15.2. the phone's operating system name and version number;
- 3.15.3. the user's IP address;
- 3.15.4. the signed document, including
  - 3.15.4.1. the title of the envelope (i.e. container) to be signed;
  - 3.15.4.2. the whole document;
  - 3.15.4.3. the signer's certificate information.

3.16. Upon launching the RIA DigiDoc mobile application, the following data will be transmitted **to the trusted list holder**, which is the Information System Authority (sr.riik.ee), **for loading the Estonian Trusted List**:
- 3.16.1. RIA DigiDoc mobile application version number;
- 3.16.2. the phone's operating system name and version number;
- 3.16.3. the user's IP address.

4. INFORMATION SYSTEM AUTHORITY'S LOGS

4.1. Upon using the ID software, the timestamp, Mobile-ID, and Smart-ID inquiries specified in clauses 3.3–3.5, 3.11–3.13 are executed through RIA'S information systems, where they are logged.
4.2. RIA also logs the inquiries specified in clauses 3.1, 3.6–3.9, 3.14-3.16.
4.3. RIA maintains the logs for 1 year.
4.4. Log data is released by law, for example to the data subject at their request, with their consent, or on any other statutory basis (for example, to a law enforcement authority in criminal proceedings).