

Privacy policy basic and trust register

1. General information

Your data is a matter of trust for us. It goes without saying that the Federal Administration only collects personal data that is absolutely necessary for the fulfillment of its tasks (data minimization). Stored data is carefully managed and protected against misuse of any kind.

Based on Article 13 of the Swiss Federal Constitution and the data protection provisions of the Confederation, every person is entitled to protection of their privacy and protection against misuse of their personal data. The Federal Administration with these provisions on its websites and web services.

2. Introduction

In this data protection declaration, the Federal Office of Information Technology and Telecommunication (FOITT) explains to what extent it processes personal data for what purpose and under what conditions with regard to the use of the basic and trust register. The FOITT processes the incoming data either under its own responsibility in accordance with this data protection declaration or by forwarding it to third parties.

[Swiss data protection law](#) regulates the processing of personal data by the Federal Administration. It applies to data processing in connection with the E-ID and the operation of associated information systems for issuing and verifying digital certificates of the Confederation's trust infrastructure. The FOITT's data processing is based on the draft Federal Act on Electronic Identity (EID Act).

3. Scope of application

This privacy policy applies to data processing in connection with the basic register and the trust register for the E-ID.

4. Person responsible

The Federal Office of Information Technology and Telecommunication FOITT is responsible for the data processing here

3003 Berne

Switzerland

T +41 58 463 25 11

info@bit.admin.ch

5. Data processing and purpose Basic register and trust register

The Federal Office of Information Technology and Telecommunications (FOITT) provides a publicly accessible basic register; this contains data that is required:

- to check whether the electronic evidence such as cryptographic keys and identifiers have been subsequently changed;
- to check whether the electronic proofs originate from the issuers entered in the basic register and the corresponding identifiers;
- for the entry of persons in the trust register who issue (issuers) or verify (verifiers) electronic certificates;
- to check whether an electronic proof has been revoked.

The basic register does not contain any data on the individual electronic certificates, with the exception of data on their revocation. The data on the revocation of electronic certificates does not allow any conclusions to be drawn about the identity of the or the content of the certificate.

The FOITT a publicly accessible trust register; this contains data that is useful for:

- verification of the identity provided by the issuers and verifiers;
- the secure use of electronic evidence.

We process the following personal data when you use our website:

- Name
- First name
- E-mail address
- IP address

6. The registration provides for the following processing steps (onboarding):

6.1 Verification via the Base Register (Technical Trust)

People register on the E-ID page in the ePortal with their surname, first name and e-mail address. Registered persons then receive access to the API Selfservice Portal in the UI interface, where they can enter their DID. The DID is authorized in the controller and then stored in the base register.

6.2 Authorization through a trust statement in the Trust Registry (Human Trust)

Users register in the ePortal and from there access the Swiyu application. In the Swiyu application, users register their organizations as business partners. This gives them access to the interfaces provided by the BIT in the API Selfservice Portal, which is also accessible via the ePortal. In the API Selfservice Portal, users can subscribe to the APIs and carry out their DID management. Users then send the keys to the FOITT by e-mail so that the FOITT can add them manually to the Trust Registry.

7. What happens to your data?

The processing of personal data on federal websites is limited to the data required to provide a functional website and user-friendly content and services or to the data that you have actively provided to us. The personal data we collect will only be stored for as long as is necessary to fulfill the respective purpose. Legal requirements or other obligations may lead to longer storage.

8. Duration of storage

Base and trust register

The following data contained in the information system will be destroyed after expiry of the following deadlines:

- the data on the E-ID applied for and issued as well as the information on the revocation of the E-ID: 20 years after the date of application or issue;
- the data on the issuing process, including the biometric data referred to in Article 16 paragraph 3, which are necessary to investigate the fraudulent use of an E-ID: five years after the expiration date of the E-ID.

- All other data is destroyed 90 days after it has been entered into the system. The archiving regulations of the Confederation are reserved.

G. Data transfer

In order to achieve the purposes described in this privacy policy, it may be necessary for us to pass on your personal data to other authorities or service providers. These are the following categories of recipients:

- external service providers;
- Suppliers;
- Authorities;
- Courts, if applicable.

The provision of reports from the information systems or their retrieval via the ePortal takes place via servers of the Federal Administration.

10. Place of data processing

We only store and process your personal data in Switzerland.

11. Data security

The FOITT takes appropriate security precautions of a technical nature (e.g. encryption, logging, access controls and restrictions, data backup, IT and network security solutions, etc.) and organizational nature (e.g. instructions to employees, confidentiality agreements, checks, etc.) to protect data from unauthorized access, loss and misuse.

Website: When you visit the website, the Federal Administration uses encrypted data communication based on TLS in conjunction with the highest level of encryption supported by your browser. You can check whether an individual page of the website is transmitted in encrypted form by the closed display of the key or lock symbol in the address bar of your browser.

General data processing: In addition, the Federal Administration applies suitable technical and organizational security measures when processing data in order to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or unauthorized access by third parties.

The Federal Administration's security measures correspond to the current state of the art.

12. Your rights in relation to your personal data

You have the following rights in relation to personal data concerning you:

- The right to receive information about what personal data we store about you and how we process it;
- the right to receive or transfer a copy of your personal data in a commonly used format;
- the right to rectification of your personal data;
- the right to erasure of your personal data;
- and the right to object to the processing of your personal data.

Please note that legal requirements and exceptions apply to these rights. To the extent permitted by law, we may refuse your request to exercise these rights. You also have the right to lodge a complaint with the competent data protection supervisory authority.

13. Changes

The FOITT may amend this privacy policy at any time without prior notice, in particular if we change our data processing or if new legal provisions become applicable. The current published version or the version valid for the respective period shall apply.