Federal Act on the Surveillance of Post and Telecommunications (SPTA)

of 18 March 2016 (Status as of 1 May 2022)

The Federal Assembly of the Swiss Confederation,

based on Articles 92 paragraph 1 and 123 paragraph 1 of the Federal Constitution[1], and having considered the Federal Council dispatch dated 27 February 2013[2],

decrees:

Section 1 General Provisions

Art. 1 Material scope of application

1 This Act applies to the surveillance of post and telecommunications ordered and carried out:

a. in the course of criminal proceedings;

b. in execution of a request for mutual legal assistance;

c. in the search for missing persons;

d. in tracing persons on whom a custodial sentence or custodial measure has been imposed;

e.[3] within the scope of the Intelligence Service Act of 25 September 2015[4] (IntelSA).

2 For information on payment transactions subject to the Postal Services Act of 17 December 2010[5] (PostA), the provisions on the duties to testify and to provide information to an authority apply.

AS **2018** 117

1 SR **101**
2 BBl **2013** 2683
3 See Art. 46 No 1.
4 SR **121**
5 SR **783.0**

Art. 2 Personal scope of application

This Act establishes duties to cooperate for the following persons and entities (entities obliged to cooperate):

a. providers of postal services under the PostA[6];

b. providers of telecommunications services under Article 3 letter b of the Telecommunications Act of 30 April 1997[7] (TCA);

c. providers of services which are based on telecommunications services and enable one-way or multipath communication (providers of derived communications services);

d. operators of internal telecommunications networks;

e. persons who grant third parties access to a public telecommunications;

f. professional retailers of cards and similar means which permit access to a public telecommunications network.

Art. 3 Surveillance service

[1] The Confederation shall operate a service for the surveillance of post and telecommunications under Article 269 of the Swiss Criminal Procedure Code[8] (CrimPC) (the Service).

[2] The Service shall perform its tasks autonomously. It is not subject to instructions and is only administratively assigned to the Federal Department of Justice and Police (FDJP).

[3] The licensing and supervisory authorities responsible for matters of post and telecommunications, the prosecution authorities and the Service work together in its area of responsibility.

Art. 4 Processing personal data

The Service, the ordering authorities, the approving authorities and the providers of postal and telecommunications services may process the personal data, including sensitive personal data and personality profiles, that they need to order, approve and carry out surveillance.

Art. 5 Advisory body

[1] The FDJP may set up an advisory body comprising representatives of the FDJP, the Service, the cantons, the prosecution authorities, the Federal Intelligence Service (FIS) and the providers of postal and telecommunications services.[9]

[2] The advisory body shall facilitate an exchange of experiences and opinions between the representatives referred to in paragraph 1. It shall examine revisions to

6 SR **783.0**
7 SR **784.10**
8 SR **312.0**
9 See Art. 46 No 1.

this Act and the implementing provisions and changes in official practice in order to promote the proper conduct of surveillance and continuous further development in this area. It shall express its opinion on draft revisions and may make recommendations on its own initiative.

[3] The FDJP shall regulate the composition and organisation of the advisory body and the procedures it has to follow.

Section 2
Information System for Processing Data from Telecommunications Surveillance

Art. 6 Principle

The Service shall operate an information system for processing the data arising from telecommunications surveillance under Article 1 paragraph 1 (the processing system).

Art. 7 Purpose of the processing system

The processing system serves to:

a. receive the data collected by telecommunications surveillance and make it available to the authorised authorities;

b. maintain over an extended period the legibility and security of the data collected by telecommunications surveillance;

c. provide information on access to telecommunications services;

d.[10] offer processing functions for the data stored in the system, including analysis functions such as visualisation, alerting or speaker recognition;

e. support business processing and controls.

Art. 8 Content of the processing system

The processing system holds:

a. the content of communications to and from the person under surveillance;

b. the data that indicates with whom, when, for how long, and from where the person under surveillance is or has been communicating, as well as the technical characteristics of the communication concerned (secondary telecommunications data);

c. information on telecommunications services;

10 Amended by No I of the FA of 1 Oct 2021 (Amendment of Legislation on Using Data in the PTSS Processing System), in force since 1 May 2022 (AS **2022** 190; BBl **2020** 6985).

d.[11] the data, in particular the personal data, required by the Service for business processing and control and for processing functions;

e.[12] results from the processing of data that is collected during telecommunications surveillance under this Act, including analysis such as visualisation, alerting or speaker recognition.

Art. 9 Access to the processing system

[1] The Service shall grant online access to the data collected in the proceedings in question to the authority that ordered surveillance or which later directs the proceedings and to the persons designated by that authority.

[2] The authority referred to in paragraph 1 and the persons it designates shall have access to such data for as long as the authority is responsible for the proceedings.

[3] If the authority transfers the proceedings to a different authority, or if it concludes the proceedings, it shall notify the Service. It shall notify the Service of the new authority that is responsible for the proceedings.

[4] The data collected by surveillance shall be sent by post to the authority at its request, if possible in encrypted form, by means of data carriers or documents, if:

a. it is intended to transmit the data to a foreign authority in an international mutual legal assistance procedure; or

b. online access is not possible for technical reasons.

Art. 10 Right to inspect case documents and right to information on the data

[1] In the case of data collected in the course of criminal proceedings or in connection with the execution of a request for mutual legal assistance:

a. the right to inspect case documents and the right to information in pending proceedings is governed by the applicable procedural law;

b. the right to information after the conclusion of the proceedings is governed by the Federal Act of 19 June 1992[13] on Data Protection (FADP) if a federal authority is dealing with the request for mutual legal assistance, or by cantonal law if a cantonal authority is dealing with it.

[2] The right to information on the data collected in the search for missing persons or tracing convicted persons is governed by the FADP if a federal authority is responsible for the search or for tracing, or by cantonal law if a cantonal authority is responsible for it. Article 279 CrimPC[14] applies *mutatis mutandis*.

11 Amended by No I of the FA of 1 Oct 2021 (Amendment of Legislation on Using Data in the PTSS Processing System), in force since 1 May 2022 (AS **2022** 190; BBl **2020** 6985).
12 Inserted by No I of the FA of 1 Oct 2021 (Amendment of Legislation on Using Data in the PTSS Processing System), in force since 1 May 2022 (AS **2022** 190; BBl **2020** 6985).
13 SR **235.1**
14 SR **312.0**

[2bis] The right to information on the data collected in implementing the IntelSA[15] is governed by the IntelSA.[16]

[3] The person affected by surveillance may assert his or her rights against the authority responsible for the proceedings or, if there is no authority that is still responsible for the proceedings, against the last authority responsible. The Service is not responsible for providing the information.

[4] The Federal Council shall regulate the manner in which these rights are granted. In doing so, it shall guarantee the rights of the parties concerned, in particular in cases where making copies of the case files is impossible or only possible with disproportionate effort.

Art. 11 Retention period for the data

[1] The length of time that data collected in criminal proceedings must be retained in the processing system is governed by the rules on criminal case files under the applicable criminal procedural law.

[2] The data collected in execution of a request for mutual legal assistance shall be retained in the processing system for as long as necessary for the objective pursued, but no longer than 30 years after conclusion of surveillance.

[3] The data collected as part of the search for a missing person shall be retained in the processing system for as long as necessary for the objective pursued, but no longer than 30 years after conclusion of surveillance.

[4] The length of time that data collected in tracing a person on whom a custodial sentence has been imposed must be retained in the processing system is governed by the applicable criminal procedural law. Data collected in tracing a person on whom a custodial measure has been imposed must be retained in the processing system for as long as necessary for the objective pursued, but no longer than 30 years after conclusion of surveillance.

[4bis] The data collected in implementing the IntelSA[17] shall be retained in the processing system for as long as necessary for the objective pursued, but no longer than 30 years after conclusion of surveillance.[18]

[5] The authority responsible for the proceedings or, if if there is no authority that is still responsible for the proceedings any longer, the last authority responsible is responsible for compliance with the periods laid down in paragraphs 1–4. It shall inform the Service before expiry of the retention period as to what is to be done with the data under the applicable law prior to its deletion from the system. Thirty years after conclusion of surveillance, the Service shall request the authority to clarify what is to be done with the data still available in the system.

15 SR **121**
16 See Art. 46 No 1.
17 SR **121**
18 See Art. 46 No 1.