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.

[6] The Federal Council shall specify how compliance with the retention periods is to be guaranteed; it shall regulate the details of the information according to paragraph 5.

Art. 12 Security

[1] The Service is responsible for the security of the processing system.

[2] The Federal Council shall issue regulations on technical and organisational protection measures, in particular against the unintentional or unauthorised access to data and the unintentional or unauthorised modification, dissemination or destruction of data.

[3] When delivering the data collected by surveillance, the entities obliged to cooperate are responsible for data security up to the point at which the Service receives the data. They shall follow the instructions of the Service regarding data security.

Art. 13 Responsibility

The authorities with access to the processing system under Article 9 are deemed to be the controller of the data file in the case of data from surveillance measures within their area of responsibility.

Art. 14 Interface with the police information systems of the Federal Office of Police

[1] The data contained in the processing system may be copied to the information systems referred to in Articles 10, 12 and 13 of the Federal Act of 13 June 2008[19] on the Federal Police Information Systems (FPISA) using the online access, provided:

a. the applicable law allows data processing in these systems; and

b. it is ensured that only those persons responsible for the relevant proceedings have access to the data.

[2] The data may only be transmitted by a person who has access rights to the processing system pursuant to this Act and to the relevant information system pursuant to the FPISA.

Art. 14*a*[20] Interface to the FIS information system

[1] The data contained in the processing system may be copied to the information system referred to in Article 58 IntelSA[21] using the online access, provided:

a. the applicable law allows data processing in this system; and

b. it is ensured that only the persons responsible for the relevant surveillance measure have access to the data.

19 SR **361**
20 See Art. 46 No 1.
21 SR **121**

[2] The transmission may only be initiated by a person who has access rights to the processing system pursuant to this Act and to the relevant information system pursuant to the IntelSA.

Section 3 Tasks of the Service

Art. 15 Information on telecommunications services

[1] The Service shall provide only the following authorities with information on the data referred to in Articles 21 and 22, on request and only for the following purposes:

a. the federal and cantonal authorities that have the right to order or approve telecommunications surveillance, or the authorities designated by them: for the purpose of determining the services and persons to be placed under surveillance and the persons communicating with them;

b. the Federal Office of Police and the cantonal and communal police authorities: for the purpose of carrying out police duties;

c. the competent federal and cantonal authorities: for the purpose of processing cases under administrative criminal law;

d.[22] the FIS: for the purpose of fulfilling tasks under the IntelSA[23].

[2] Furthermore, pursuant to Articles 10 paragraph 3 and 23 of the Federal Act of 19 December 1986[24] on Unfair Competition (UCA), the Service shall also provide the competent federal authority on request with information on the data referred to in Article 21 in order that the authority may file a criminal complaint of unfair competition pursuant to Article 3 paragraph 1 letter u UCA.[25]

Art. 16 General tasks related to surveillance

In relation to surveillance of post and telecommunications, the Service has the following general tasks:

a. It shall contact the ordering authority and the approving authority immediately before post or information is passed on to the ordering authority if, in its opinion, the surveillance order:

1. in the case of surveillance in the course of criminal proceedings, does not concern a criminal offence for which surveillance is permitted under the applicable law;

2.[26] has not been issued by the competent authority or, pursuant to Articles 29–31 IntelSA[27], has not been approved and granted permission to proceed; or

22 See Art. 46 No 1.
23 SR **121**
24 SR **241**
25 See Art. 46 No 1.
26 See Art. 46 No 1.

3. is incomplete or unclear.

b. It shall contact the ordering authority and the approving authority immediately if, in its opinion, the surveillance is technically inappropriate, does not correspond to the surveillance types provided for by law or in the implementing provisions or is not technically feasible.

c. It shall provide the competent authority with the information required to order surveillance; if necessary, it shall request the entities obliged to cooperate to provide it with this information.

d. It shall instruct the entities obliged to cooperate on how to carry out the surveillance, request them to take the necessary measures for the surveillance and supervise the implementation of the surveillance.

e. It shall implement the measures ordered by the approving authority to protect professional secrecy.

f. It shall check whether surveillance extends beyond the approved period and terminate it at the end of the period if it has not been sent a copy of the renewal application.

g. It shall notify the approving authority immediately of the termination of surveillance.

h. It shall follow the technical developments in relation to postal and telecommunications services.

i. It shall organise and carry out training for persons who are allowed to access the processing system.

j. It may, on request, advise authorities and entities obliged to cooperate on technical, legal and operational aspects of surveillance of post and telecommunications.

k. It shall produce statistics on surveillance.

Art. 17 Tasks related to telecommunications surveillance

In relation to telecommunications surveillance, the Service has the following additional tasks:

a. If several providers of telecommunications services are involved in providing the telecommunications service to be placed under surveillance, the Service shall instruct the provider responsible for the administration of the telecommunications service or the provider that can conduct the surveillance with the least technical effort to carry out the surveillance. The Service shall base its instructions on the information provided by the authority that ordered the surveillance.

b. It shall receive the transmitted telecommunications of the person under surveillance from the providers of telecommunications services, store them and

27 SR **121**

allow the ordering authority or the authority designated by the ordering authority to have access thereto.

c. It shall instruct the providers of telecommunications services to transmit data collected in the course of surveillance directly to the ordering authority (direct transmission) or the authority designated by the ordering authority if, for technical reasons, it is not able to receive the telecommunications, to store them or to give access to these authorities; in such an event, these authorities shall store the data themselves.

d. It shall receive the secondary telecommunications data of telecommunications from providers of telecommunications services, store it, and give access to the ordering authority or the authority designated by the ordering authority.

e. In cases where the entities obliged to cooperate are merely subject to an obligation of toleration and cooperation (Arts. 26 para. 6, 27 paras. 1 and 2, 28 and 29) or where non-standardised surveillance is to be carried out (Art. 32 para. 2), it shall take the steps required to ensure that surveillance can still be carried out.

f. It shall verify the ability of providers of telecommunications services to provide information and conduct surveillance (Arts. 32–34).

g. At the request of the ordering authority, it shall filter certain data types out of the data flow.

Art. 18 Quality control

[1] The Service shall take preventive and retrospective measures for quality control of the data delivered by the providers of telecommunications services.

[2] It may only view the content of the data with the prior consent of the authority responsible for the proceedings.

Section 4 Obligations related to Post Surveillance

Art. 19 Obligations of providers of postal services

[1] At the request of the Service, providers of postal services must deliver to the ordering authority or to the authority designated by the ordering authority:

a. the post addressed to or mailed by the person under surveillance;

b. the data that indicates with whom, when and from where the person under surveillance is or was communicating, as well as the technical characteristics of the post concerned (secondary data of postal services).

[2] The order may require real-time surveillance to be carried out and the handover of the retained secondary data of postal services from past communications (retroactive surveillance).

[3] The Federal Council shall specify the permissible types of surveillance and shall regulate for each type of surveillance the data to be supplied by the various providers.

[4] Providers must retain the secondary data of postal services specified by the Federal Council on the basis of paragraph 3 for 6 months.

[5] Subject to the prior consent of the authority responsible for the proceedings, the post concerned shall be returned to the provider, which shall deliver it to the person under surveillance.

Art. 20 Information before ordering surveillance

Providers of postal services must provide the Service, at its request, with the information required for ordering surveillance.

Section 5 Information relating to Telecommunications Surveillance

Art. 21 Information on telecommunications services

[1] Providers of telecommunications services shall supply the Service with the following information on specified telecommunications services:

a. the surname, first name, date of birth, address and, if known, the occupation of the subscriber;

b.[28] the addressing resources under Article 3 letter f of the Telecommunications Act of 30 April 1997[29] (TCA);

c. the types of services;

d. other data on telecommunications services specified by the Federal Council; such data may be administrative or technical in nature or permit the identification of persons;

e. in addition in the case of customer relationships for pre-paid or free services: the place of supply and the surname and first name of the person who supplied the means of access to the telecommunications service.

[2] They must ensure that this information is recorded when the customer relationship is established and can be supplied during the customer relationship and for 6 months after its termination. The Federal Council shall specify that the providers of telecommunications services must retain and be able to supply certain of these data for the purpose of identification for only 6 months.

28 Amended by Annex No 4 of the FA of 22 March 2019, in force since 1 Jan. 2021 (AS **2020** 6159; BBl **2017** 6559).
29 SR **784.10**

Art. 22 Information to identify perpetrators of criminal offences via the internet and to identify persons in the case of threats to internal or external security[30]

[1] If it is suspected that a criminal offence has been committed via the internet, providers of telecommunications services are required to provide the Service with all the information necessary to identify the perpetrator.

[1bis] If sufficient evidence exists that a threat to internal or external security is being or has been made via the internet, providers of telecommunications services are required to provide the Service with all the information required to identify the author of the threat or the origin of the threat.[31]

[2] The Federal Council shall determine which information the providers of telecommunications services must retain and be able to supply for the purpose of identification during the customer relationship and for 6 months after its termination. It shall specify certain of these data that providers of telecommunications services must retain and be able to supply for the purpose of identification for only 6 months. Providers of telecommunications services must provide the Service with further information available to them.

[3] Providers of derived communications services and operators of internal telecommunications networks must provide the Service with the information available to them.

[4] The Federal Council may require providers of derived communications services that offer services of major economic importance or to a large number of users to retain and supply all or some of the information that the providers of telecommunications services must provide under paragraph 2.

Art. 23 Procedure for recording data and providing information

[1] The Federal Council shall regulate how providers of telecommunications services must record the data pursuant to Article 21 paragraph 1 letter a and Article 22 paragraph 2 first sentence.

[2] It shall regulate the form and retention of information requests.

[3] It may provide that the data referred to in Articles 21 and 22 be made accessible online at all times to the authorities referred to in Article 15.[32]

Art. 24 Information before ordering surveillance

Providers of telecommunications services must provide the Service on its request with the technical information required for ordering surveillance.

30 See Art. 46 No 1.
31 See Art. 46 No 1.
32 Amended by No I 9 of the FA of 19 March 2021 on Administrative Facilitations and a Relief of the Federal Budget, in force since 1 Jan. 2022 (AS **2021** 654; BBl **2020** 6985).

Art. 25 Information on services

Providers of telecommunications services shall inform the Service on its request at any time in detail of the type and characteristics of the services they have placed on the market or wish to bring to the market within 6 months.

Section 6 Obligations related to Telecommunications Surveillance

Art. 26 Obligations of providers of telecommunications services

[1] Providers of telecommunications services shall on request supply the following information to the Service or, in accordance with Article 17 paragraph c, to the ordering authority or the authority designated by the ordering authority:

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

b. the secondary telecommunications data of the telecommunications to and from the person under surveillance.

[2] They must also:

a. provide the information required to carry out the surveillance;

b. tolerate surveillance carried out by the Service or by persons it designates; for this purpose they shall grant immediate access to their facilities;

c. remove any encryption they have applied.

[3] Providers of telecommunications services who are involved in providing the telecommunications service under surveillance must supply their data to the Service or to the provider instructed to carry out the surveillance.

[4] The order may require real-time surveillance to be carried out and the handover of the retained secondary telecommunications data of telecommunications from past communications (retroactive surveillance).

[5] Providers of telecommunications services must retain the secondary telecommunications data of telecommunications for 6 months.

[6] The Federal Council may exempt providers of telecommunications services from certain statutory obligations, in particular if they offer services of minor economic importance or in the field of education. It shall not exempt them from the obligation to supply on request the secondary telecommunications data of telecommunications available to them relating to the person under surveillance and the obligations referred to in paragraph 2.

Art. 27 Obligations of providers of derived communications services

[1] Providers of derived communications services must tolerate surveillance carried out by the Service or by persons it designates of the data that the person under surveillance transmits or stores using derived communications services. For this purpose, they must without delay:

a. grant access to their facilities;

b. provide the information required for the surveillance.

[2] On request, they must supply the secondary telecommunications data of telecommunications available to them relating to the person under surveillance.

[3] In so far as is necessary for telecommunications surveillance, the Federal Council shall make providers of derived communications services that provide services of major economic importance or to a large number of users subject to all or some of the obligations referred to in Article 26. In such an event, the provisions of this Act that apply to providers of telecommunications services apply *mutatis mutandis*.

Art. 28 Obligations of operators of internal telecommunications networks

[1] Operators of internal telecommunications networks must tolerate surveillance carried out by the Service or by persons it designates. For this purpose, they must without delay:

a. grant access to their facilities;

b. provide the information required for the surveillance.

[2] On request, they must supply the secondary telecommunications data of telecommunications available to them relating to the person under surveillance.

Art. 29 Obligations of persons who make their access to a public telecommunications network available to third parties

[1] Persons who make their access to a public telecommunications network available to third parties must tolerate surveillance carried out by the Service or by persons it designates. For this purpose, they must without delay:

a. grant access to their facilities;

b. provide the information required for the surveillance.

[2] On request, they must supply the secondary telecommunications data of telecommunications available to them relating to the person under surveillance.

Art. 30 Obligations of professional retailers of cards and similar means

Professional retailers of cards and similar means which permit access to a public telecommunications network must record the information referred to in Article 21 paragraph 1 and forward it to the provider of telecommunications services whose network can be accessed using the card or similar means.

Section 7
Ensuring the Ability of Providers of Telecommunications Services to provide Information and conduct Surveillance

Art. 31 Implementing provisions on types of information requests and surveillance

[1] The Federal Council shall specify the information to be provided by providers of telecommunications services and the types of surveillance they must conduct. It shall specify for each type of information request and surveillance which data must be supplied.

[2] It shall set time limits for supplying the data.

[3] The FDJP shall issue the technical and administrative provisions required for the standardised provision of information and the standardised conduct of the common types of surveillance. It shall specify, in particular, the interfaces and data formats to be used for delivering the data to the Service. It shall take account of the corresponding international standards.

Art. 32 Ability to provide information and carry out surveillance

[1] Providers of telecommunications services must at all times be able, in accordance with the applicable law, to supply the information referred to in Articles 21 and 22 and the information referred to in Articles 24 and 26 paragraph 2 letter a and to carry out surveillance of the telecommunications services they offer, provided the provision of information and the surveillance are standardised.

[2] Where information is requested or surveillance types are ordered that are not standardised, providers of telecommunications services must work with the Service in accordance with its instructions and take all appropriate measures to ensure trouble-free implementation.

[3] Providers of telecommunications services may, at their own expense, entrust third parties to fulfil these obligations. They must ensure that the third parties can guarantee the security and confidentiality of the data. Third parties entrusted with the fulfilment of these obligations shall be subject to the supervision of the Service.

Art. 33 Proof of ability to provide information and carry out surveillance

[1] At the request of the Service, providers of telecommunications services must prove at their own expense that they are able, in accordance with the applicable law, to respond to the standardised information requests and to carry out the standardised surveillance types.

[2] The Service may engage third parties to verify ability to provide information and carry out surveillance.

[3] It shall define the technical and organisational details for providing proof in individual cases.

[4] It shall charge the provider of telecommunications services a fee to cover the cost of verification. The Federal Council shall set the fees.

[5] It may instruct providers to take technical and organisational measures to remedy deficiencies related to their ability to provide information and carry out surveillance.

[6] It shall issue confirmation to the providers as soon as proof has been provided. The Federal Council shall regulate the content and term of validity of this confirmation, in particular in the case of technical advances.

Art. 34 Liability for costs in case of insufficient cooperation

[1] Providers of telecommunications services must bear the costs incurred if they are unable or unwilling to fulfil their obligations under Article 32 and these obligations must as a result be assigned to the Service or to a third party.

[2] They are not required to bear the costs if they are unable to fulfil their obligations and one of the following is true:

a. They have valid confirmation of their ability to carry out the type of surveillance concerned.

b. They have submitted proof of their ability to carry out surveillance, but this has not been verified within a reasonable period for reasons beyond their control.

Section 8 Searches for Missing and Convicted Persons

Art. 35 Search for missing persons

[1] Outside criminal proceedings, the competent authority may order surveillance of post and telecommunications in order to find a missing person.

[2] A person is considered missing if the following conditions are met:

a. his or her whereabouts are unknown or disproportionately difficult to determine; and

b. there are serious indications that his or her health or life are in grave danger.

[3] The competent authority may employ technical equipment in accordance with Article 269bis CrimPC[33], provided the previous measures for telecommunications surveillance pursuant to Art. 269 CrimPC have been unsuccessful, or a search using these measures would be futile or disproportionately difficult. It shall produce statistics on surveillance in accordance with Art. 269bis CrimPC.

[4] The competent authority may also inspect data on third parties where this appears necessary in the circumstances in order to find the missing person.

33 SR **312.0**

Art. 36 Search for convicted persons

[1] Outside criminal proceedings, the competent authority may order surveillance of post and telecommunications in order to find a person on whom a legally binding and enforceable custodial sentence or custodial measure has been imposed, provided the previous search measures have been unsuccessful or if a search would be futile or would be disproportionately difficult in the absence of surveillance.

[2] The competent authority may employ technical equipment in accordance with Article 269bis CrimPC[34] and computer programs pursuant to Article 269ter CrimPC, provided the previous measures for telecommunications surveillance pursuant to Article 269 CrimPC have been unsuccessful, or the search using these measures would be futile or disproportionately difficult. It shall produce statistics on surveillance in accordance with Article 269bis and 269ter CrimPC.

[3] It may also inspect data on third parties, provided the requirements of Article 270 CrimPC are met *mutatis mutandis*.

Art. 37 Procedure

[1] Articles 271, 272 and 274–279 CrimPC[35] apply *mutatis mutandis* to the procedure.

[2] In the case of an emergency search, the persons under surveillance shall be informed as soon as possible in derogation from Article 279 CrimPC.

[3] The Confederation and the cantons shall designate the ordering authority, the approving authority and the appeal body. A surveillance order requires approval by a judicial authority.

Section 9[36] Costs

Art. 38 Principles

[1] The entities obliged to cooperate shall bear the costs of the facilities required to fulfil their obligations under this Act.

[2] They shall receive adequate compensation from the Service for the costs that they incur in conducting surveillance and providing information pursuant to Articles 21 and 22.

[3] The cantons shall contribute the costs incurred by the Service in providing its services and paying compensation to the entities obliged to cooperate.

[4] The Federal Council may provide that:

a. the entities obliged to cooperate receive no compensation for providing any information or for providing certain information;

34 SR **312.0**
35 SR **312.0**
36 Amended by No I 9 of the FA of 19 March 2021 on Administrative Facilitations and a Relief of the Federal Budget, in force since 1 Jan. 2022 (AS **2021** 654; BBl **2020** 6985).

b. services provided by the Service in connection with the provision of any information or certain information are not taken into account in calculating the cantons' contribution to the costs.

Art. 38*a* Modalities

[1] The Federal Council shall regulate the calculation and disbursement of compensation and the calculation and collection of contributions to costs.

[2] It may provide that the compensation and contributions to costs are calculated on an individual basis or at a flat rate.

[3] It shall specify the tariffs for calculations made on an individual basis.

[4] For calculations made on a flat-rate basis, it shall take account of the extent to which the costs may be attributed to the Confederation or to individual cantons according to the benefit of the information and the surveillance. If the cantons have agreed on the shares of the overall costs that they are each to bear, the allocation of costs shall be based on this agreement.

[5] In the case of flat-rate compensation and contributions to costs, the Service shall provide statements on its services and those of the entities obliged to cooperate showing the amounts that would be incurred in the case of an individual assessment.

Section 10 Criminal Provisions

Art. 39 Contraventions

[1] Unless they have committed a more serious offence under another law, any person who wilfully:

a. fails to comply with a decision addressed to them by the Service that mentions the penalties under this Article in the time provided;

b. fails to comply with the obligation to retain data under Articles 19 paragraph 4 and 26 paragraph 5;

c. fails to comply with the obligation to record and, if necessary, pass on the required customer data (Art. 21 para. 2 and Art. 30) when establishing a customer relationship;

d. fails to preserve secrecy vis-à-vis third parties with regard to surveillance;

shall be liable to a fine not exceeding 100,000 francs.

[2] An attempt is also an offence.

[3] If the offender acts through negligence, the penalty is a fine not exceeding 40,000 francs.

Art. 40 Jurisdiction

[1] Offences under Article 39 shall be prosecuted and adjudicated in accordance with the Federal Act of 22 March 1974[37] on Administrative Criminal Law.

[2] The Service is responsible for the prosecution and adjudication.

Section 11 Oversight and Rights of Appeal

Art. 41 Oversight

[1] The Service shall oversee compliance with the legislation on surveillance of post and telecommunications.

[2] If it identifies an infringement of the law, it may take the measures referred to in Article 58 paragraph 2 letter a TCA[38] *mutatis mutandis* against providers of telecommunications services. It may order precautionary measures.

Art. 42 Rights of appeal

[1] Decisions by the Service are subject to appeal in accordance with the general provisions on federal administrative justice.

[2] The plea that the requirements for ordering the surveillance have not been met is not an admissible ground for an appeal against a decision by the Service.

[3] An appeal does not have suspensive effect except where the decision relates to a cash consideration. The appeal body may accord suspensory effect to the appeal.

Section 12 Final Provisions

Art. 43 Implementation

The Federal Council and, to the extent that they are responsible, the cantons shall issue the provisions required to implement this Act.

Art. 44 Repeal and amendment of other legislation

The repeal and amendment of other legislation are regulated in the Annex.

Art. 45 Transitional provisions

[1] Surveillance that is in progress at the time that this Act comes into force shall continue in accordance with the new law.

[2] Appeals against the Service's decisions shall be dealt with in accordance with the law applicable in the proceedings at the first instance.

37 SR **313.0**
38 SR **784.10**

[3] The obligation laid down in Article 21 paragraph 2 applies to information about prepaid SIM cards and similar means that must still be available under the previous law at the time that this Act comes into force.

[4] The compensation and fees for surveillance pursuant to this Act are governed by the law that was in force at the time surveillance was ordered.

Art. 46 Coordination with the Intelligence Service Act of 25 September 2015

Regardless of whether this Act or the Intelligence Service Act of 25 September 2015[39] *comes into effect first, the provisions below shall on the commencement of the Act that comes into force later or on commencement of both Acts at the same time be worded as follows:*

…[40]

Art. 47 Referendum and commencement

[1] This Act is subject to an optional referendum.

[2] The Federal Council shall determine the commencement date.

Commencement date: 1 March 2018[41]

39 SR **121**
40 The provisions may be consulted under AS **2018** 117.
41 FCD of 15 Nov. 2017.

Annex
(Art. 44)

Repeal and Amendment of other Legislation

I

The Federal Act of 6 October 2000[42] on the Surveillance of Post and Telecommunications is repealed.

II

The legislation below is amended as follows:

…[43]

42 [AS **2001** 3096; **2003** 3043 No I 2; **2004** 3693; **2007** 921 Annex No 3; **2010** 1881 Annex 1 No II 26, 3267 Annex No II 14; **2017** 4095 Annex No II 12]
43 The amendments may be consulted under AS **2018** 117.