Federal Act on the Intelligence Service

(Intelligence Service Act, IntelSA)

of 25 September 2015 (Status as of 1 January 2024)

The Federal Assembly of the Swiss Confederation,

on the basis of Articles 54 paragraph 1, 123 paragraph 1 and 173 paragraph 2 of the Federal Constitution[1,2]
and having considered the Federal Council Dispatch dated 19 February 2014[3],

decrees:

Chapter 1 General Provisions and Principles governing Information Gathering

Art. 1 Subject matter

This Act regulates:

a. the activities of the Federal Intelligence Service (FIS);

b. cooperation between the FIS and other federal authorities, the cantons, foreign countries and private individuals;

c. political governance of the FIS and the control and supervision of intelligence activities.

Art. 2 Aim

This Act serves to protect important national interests; its aim is

a. to contribute towards safeguarding Switzerland's democratic and constitutional principles and protecting the freedoms of its population;

b. to increase the security of the Swiss population and of Swiss citizens abroad;

AS **2017** 4095

1 SR **101**

2 Amended by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).

3 BBl **2014** 2105

c. to support Switzerland's capacity to act;

d. to contribute towards safeguarding international security interests.

Art. 3 Safeguarding further important national interests

In the event of a serious and immediate threat, the Federal Council may deploy the FIS not only to protect the national interests mentioned in Article 2 but also:

a. to protect basic constitutional order in Switzerland;

b. to support Swiss foreign policy;

c. to protect Switzerland as a location for employment, business and finance.

Art. 4 Authorities and persons subject to obligations

This Act applies to the following authorities and persons:

a. federal and cantonal authorities that are given the task of carrying out intelligence activities;

b. federal and cantonal authorities and public and private organisations, persons and entities that hold information relevant to intelligence matters;

c. private individuals who are required to pass on information relevant to intelligence matters in terms of this Act.

Art. 5 Principles governing information gathering

[1] In order to carry out its tasks, the FIS shall gather information from sources that are publicly and non-publicly accessible.

[2] For this purpose it shall use information gathering measures which do and do not require authorisation.

[3] In each case, it shall choose the information gathering measure that:

a. is most suitable and necessary for achieving a specific information gathering objective; and

b. causes the least interference with the fundamental rights of the persons concerned.

[4] It may gather personal data without this coming to the attention of the persons concerned.

[5] It may not gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland.

[6] It may by way of exception gather information in accordance with paragraph 5 about an organisation or person and record that information in relation to a person if there are specific indications that the person is exercising their rights in order to prepare for or carry out terrorist, espionage or violent-extremist activities.

7 It shall delete data recorded in relation to a person once participation in the activities mentioned paragraph 6 can be excluded, but one year at the latest after the information has been recorded if no such activities have been proven up to that time.

8 It may also gather and process information in accordance with paragraph 5 about organisations and groups on the watch list in accordance with Article 72 or their members if the threats posed by these organisations and groups can be assessed thereby.

Chapter 2 FIS Tasks and Cooperation

Section 1 Tasks, Protection and Security Measures, and Weapons

Art. 6 Tasks of the FIS

1 The FIS shall gather and process information for the following purposes:

a. the early recognition and prevention of threats to internal or external security from:
   1. terrorism,
   2. espionage,
   3. the proliferation of nuclear, biological or chemical weapons, including their delivery systems, and all civilian and military goods and technologies required to manufacture such weapons (ABC proliferation) or the illegal trade in radioactive substances, war material and other armaments,
   4.[4] attacks on supply systems for energy and drinking water, information, communication and transport infrastructures and other processes, systems and facilities that are essential for the proper functioning of the economy and well-being of the population (critical infrastructures),
   5. violent extremism;

b. to identify, observe and assess events outside Switzerland that are of security-policy significance;

c. to safeguard Switzerland's capacity to act;

d. to safeguard other important national interests in accordance with Article 3 where the Federal Council has issued a specific mandate to do so.

2 The FIS shall assess the threat situation and inform the federal agencies and cantonal executive authorities concerned regularly about any threats and about the measures taken and planned in terms of this Act. If required, it shall alert the state agencies responsible.

3 It shall, while protecting its sources, inform other federal and cantonal agencies about events and intelligence that are relevant to the statutory tasks of these agencies in safeguarding internal or external security.

4 Amended by Annex 1 No 2 of the Information Security Act of 18 Dec. 2020, in force since 1 Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).

4 It shall cultivate intelligence relations between Switzerland and foreign agencies.

5 It is responsible for providing the intelligence early warning in order to protect critical infrastructures.

6 It runs programmes to provide information on and raise awareness of threats to internal or external security.

7 It protects its employees, its facilities, its sources and the data that it processes.

Art. 7 Protective and security measures

1 The FIS shall take measures to guarantee the protection, safety and security of its employees, facilities and the data that it processes. To this end it may:

a. carry out on its premises bag and personal checks on:
   1. FIS employees,
   2. persons working temporarily for the FIS,
   3. employees of companies that provide the FIS with services on its premises;

b. carry out checks of rooms and spaces in FIS facilities to verify whether the regulations on protecting classified information are being complied with;

c. monitor archive rooms, strong rooms and storerooms and the access zones to the FIS premises using video transmission and recording devices;

d. operate telecommunications jammers in accordance with Article 34 paragraph 1ter of the Telecommunications Act of 30 April 1997[5] on premises that it uses.

2 The FIS shall operate a secure computer network for its information systems that must in particular be protected against access by unauthorised persons.

Art. 8 Weapons

1 FIS employees may be issued with weapons for operations in Switzerland if they are exposed to special dangers in the course of their service duties.

2 Armed employees may only use their weapons for self-defence or in emergencies and only in a manner appropriate to the circumstances.

3 The Federal Council shall determine the categories of employee that may carry weapons and the training that they require.

5 SR **784.10**

Section 2 Cooperation

Art. 9 Cantonal executive authorities

[1] Each canton shall designate an authority to work with the FIS in implementing this Act (the cantonal executive authority). It shall ensure that this authority is able to carry out FIS assignments immediately.

[2] The FIS shall issue assignments to the cantonal executive authorities in writing; in cases of urgency it may issue assignments verbally and confirm them retrospectively in writing.

Art. 10 Informing the cantons

[1] The Federal Department of Defence, Civil Protection and Sport (DDPS) shall inform the inter-cantonal conferences of governments regularly and in the event of incidents about its assessment of the threat situation.

[2] The FIS shall inform the cantonal executive authorities about events that affect the tasks that they carry out.

Art. 11 Cooperation with the Armed Forces

[1] The FIS shall notify the responsible agencies in the Armed Forces Intelligence Service and the Military Security Service about events that affect the tasks that they carry out.

[2] It may work with the responsible agencies of the Armed Forces in relation to international military contacts, request them for information and issue them with assignments related to international cooperation.

[3] The Federal Council shall regulate:

a. the cooperation and exchange of information between the FIS and the responsible agencies of the Armed Forces Intelligence Service;

b. the division of tasks between the FIS and the Military Security Service during peace support or civil support operations or active service.

Art. 12 Cooperation with other countries

[1] The FIS may work with foreign intelligence services and security services in terms of Article 70 paragraph 1 letter f in order to implement this Act, in that it:

a. receives or passes on useful information;

b. holds joint technical discussions and conferences;

c. carries out joint activities to gather and evaluate information and to assess the threat situation;

d. procures and passes on information to the requesting state in order to assess whether a person may work on classified foreign projects related to internal

or external security or have access to classified foreign information, materials or facilities;

e. participates in terms of Article 70 paragraph 3 in international automated information systems.

2 It may in consultation with the Federal Department of Foreign Affairs (FDFA) post employees to Swiss representations abroad in order to promote international contacts. These employees shall work directly with the responsible authorities of the host state and third countries in order to implement this Act.

3 The FIS is responsible for cooperation with foreign intelligence services in order to carry out intelligence tasks in terms of this Act.

4 The cantons may work with the competent foreign police authorities in order to deal with security issues in the border zone.

Chapter 3 Information Gathering

Section 1 Information Gathering Measures not requiring Authorisation

Art. 13 Public sources of information

Public sources of information are in particular:

a. publicly accessible media;

b. publicly accessible registers of federal and cantonal authorities;

c.[6] personal data made publicly accessible by private individuals;

d. statements made in public.

Art. 14 Observation of public in generally accessible locations

1 The FIS may observe and make sound and image recordings of events and facilities in public and generally accessible locations. It may use aircraft and satellites for this purpose.

2 The observation and sound and image recording of events and facilities that fall within the private domain are not permitted. Sound and image recordings that fall within the protected private domain but which cannot be prevented for technical reasons must be destroyed immediately.

Art. 15 Human sources

1 Human sources are persons who:

a. provide the FIS with information or intelligence;

6 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

b. provide the FIS with services that assist in the fulfilment of tasks in terms of this Act;

c. support the FIS in procuring information.

2 The FIS may pay human sources appropriately for their activities. Where this is necessary in order to protect the sources or to gather further information, the payment shall not be regarded as taxable income or as income in terms of the Federal Act of 20 December 1946[7] on Old-Age and Survivors' Insurance.

3 The FIS shall take the measures required to protect the life and limb of human sources. Such measures may also be taken in respect of persons closely associated with human sources.

4 The Head of the DDPS may in specific cases authorise the FIS to provide human sources with a cover story or an alias identity on conclusion of their cooperation, if this is necessary in order to protect the life and limb of the persons concerned.

5 The measures mentioned in paragraphs 3 and 4 are limited to the period of actual danger. By way of exception, a time limit may be dispensed with or a temporary measure may be changed into a permanent measure if the risks to the persons concerned are particularly serious and it must be expected that they will continue to apply.

Art. 16 Alerts on persons and property

1 The FIS may arrange for alerts to be issued in the computerised police search system in accordance with Article 15 paragraph 1 of the Federal Act of 13 June 2008[8] on the Federal Police Information Systems (FPISA) and in the national part of the Schengen Information System in accordance with Article 16 paragraph 2 FPISA in respect of persons and vehicles.

2 An alert in respect of a person or a vehicle is only permitted if there is reason to believe that:

a. the person concerned poses a specific threat to internal or external security in accordance with Article 6 paragraph 1 letter a;

b. the vehicle is being used by a person defined in letter a;

c. the vehicle will be used for a different specific threat to internal or external security in accordance with Article 6 paragraph 1 letter a;

d. the whereabouts of a person or a vehicle must be established in order to safeguard other important national interests in accordance with Article 3.

3 The alert may not be issued in order to monitor the vehicle of a third party that belongs to any of the professions mentioned in Articles 171–173 of the Criminal Procedure Code (CrimPC)[9].

7 SR **831.10**
8 SR **361**
9 SR **312.0**

Section 2 Cover Stories and Alias Identities

Art. 17 Cover story

[1] The Director of the FIS may authorise FIS employees to be provided with a cover story so that they are not recognised as belonging to the FIS.

[2] In consultation with or at the request of a canton, the Director may also authorise members of the cantonal executive authorities to be provided with a cover story by the FIS.

[3] In order to establish and maintain a cover story, the FIS may produce or alter official documents. The responsible federal, cantonal and communal authorities are required to cooperate with the FIS.

[4] The Director of the FIS shall submit a report each year to the Head of the DDPS on the use of cover stories.

[5] Concealing one's association with the FIS or a cantonal executive authority without using official documents produced or altered for this purpose does not require any special authorisation.

Art. 18 Alias identities

[1] The Head of the DDPS may authorise the following persons to be provided with an alias identity, i.e. be given an identity other than their true identity in order to ensure their safety or facilitate information gathering:

a. FIS employees;

b. in consultation with or at the request of the canton, employees of the cantonal executive authorities acting in terms of a federal mandate;

c. human sources in the course of a specific operation.

[2] The alias identity may be used for as long as required to ensure the safety of the person concerned or facilitate information gathering. Use is subject to the following time limits:

a. for employees of the FIS or of cantonal security agencies: a maximum of five years; if required, this period may be extended for a maximum of three further years in any given case;

b. for human sources: a maximum of twelve months; if required, this period may be extended for a maximum of twelve further months in any given case.

[3] The use of an alias identity to gather information is only permitted for a purpose set out in Article 6 paragraph 1 and where:

a. attempts to gather information without using an alias identity have been unsuccessful, would have no prospect of success without the use of an alias identity or would be disproportionately more difficult; or

b. there is a threat to a significant legal interest such as the life and limb or physical integrity of the person required to gather the information or of a person closely associated with that person.

4 In order to develop and maintain a cover story, the FIS may produce or alter identity documents, official documents and other documents as well as personal details. The responsible federal, cantonal and communal authorities are required to cooperate with the FIS.

5 The FIS shall take the required measures to protect the person's true identity from being revealed.

Section 3 Duties to provide Information and to report

Art. 19 Obligation to provide information in the case of a specific threat

1 Federal and cantonal authorities and organisations that the Confederation or the cantons have mandated to fulfil public tasks are obliged in specific cases and on justified request to provide the FIS with the information required to identify or repel a specific threat to internal or external security or to safeguard other important national interests in accordance with Article 3.

2 A specific threat to internal or external security is established if a significant legal interest such as the life and limb or the liberty of persons or the existence and functioning of the state is affected and the threat comes from:

a. terrorist activities in the sense of attempts to influence or change the framework of the state that are realised or encouraged by committing or threatening to commit serious offences or by spreading fear and alarm;

b. espionage in terms of Articles 272–274 and 301 of the Criminal Code (SCC)[10] and Articles 86 and 93 of the Military Criminal Code of 13 June 1927[11];

c. ABC proliferation or the illegal trade in radioactive substances, war material and other armaments;

d. an attack on critical infrastructure; or

e. violent extremist activities in the sense of efforts by organisations that reject democratic and constitutional values and which commit, incite or endorse acts of violence in order to achieve their objectives.

3 The authorities and organisations mentioned in paragraph 1 are required to preserve secrecy in relation to third parties with regard to the request and any information provided. They are permitted to inform their superiors and supervisory bodies.

4 They may file a report without having to be requested to do so if they identify a specific threat to internal or external security in terms of paragraph 2.

5 The Federal Council shall specify in an ordinance the organisations that are required to provide information; these include in particular public and private organisations that do not form part of the Federal Administration but which issue legislation or first-instance rulings as defined in Article 5 of the Administrative Procedure Act of 20

10 SR **311.0**
11 SR **321.0**

December 1968[12] or which fulfil executive tasks that have been delegated to them by the Confederation; the cantons are not regarded as such organisations.

Art. 20 Special obligation to provide information and report

[1] The following authorities are obliged to provide the FIS with information in order to carry out its tasks:

a. courts, prosecution authorities and authorities responsible for executing criminal sentences and measures;

b. the border guard and customs authorities;

c. authorities responsible for military security, the authorities of the Armed Forces Intelligence Service and the authorities responsible for the military service registration system;

d. federal and cantonal authorities responsible for matters relating to the entry and residence of foreign nationals and for asylum matters;

e. authorities that are involved in security policing tasks;

f. residents' register offices;

g. authorities responsible for diplomatic and consular matters;

h. authorities responsible for authorising dealings with certain goods;

i. authorities responsible for the operation of computer systems;

j. authorities that are responsible for the supervision of the financial markets and for accepting reports of suspicions of money laundering in cases of financing terrorism and ABC proliferation activities in accordance with the Anti-Money Laundering Act of 10 October 1997[13].

[2] The authorities listed in paragraph 1 are required to preserve secrecy in relation to third parties with regard to the request and any information provided. They are permitted to inform their superiors and supervision bodies.

[3] The authorities listed in paragraph 1 shall file a report without having to be requested to do so if they identify a specific and serious threat to internal or external security.[14]

[4] The Federal Council shall specify in an unpublished list which activities and intelligence must be reported to the FIS without a request being required. It shall specify the extent of the obligation to report and the procedure for providing information.

Art. 21 Professional confidentiality

In the case of information in terms of Article 19 or 20, the statutory protection for professional confidentiality continues to apply.

12 SR **172.021**
13 SR **955.0**
14 The correction of the FA Drafting Committee of 12 March 2020, published 24 March 2020, relates to the French text only (AS **2020** 1057).

Art. 22 Procedure in the event of differences of opinion about obligations to provide information and to report

[1] In the event of any differences of opinion between the FIS and another unit of the Federal Administration with regard to an obligation to provide information in accordance with Article 19 or 20, the relevant joint supervisory authority shall make the final decision.

[2] In the case of differences of opinion between the FIS and an organisation, officer or authority that does not form part of the Federal Administration with regard to an obligation to provide information in accordance with Article 19 or 20, the Federal Administrative Court shall decide in accordance with Article 36*a* of the Administrative Court Act of 17 June 2005[15].

Art. 23 Reports and information from third parties

[1] The FIS may accept reports from any person.

[2] It may obtain by written or verbal request specific information that it requires in order to carry out its tasks. It may invite persons in writing to be questioned.

[3] It shall notify the person requested for information that they are providing information voluntarily; the foregoing does not apply to information gathering while using a cover story.

Art. 24 Identification and questioning of persons

[1] In order to carry out its tasks in accordance with Article 6 paragraph 1 letter a, the FIS may have a person stopped in order to establish their identity and to question them briefly in accordance with Article 23.

[2] The person shall be stopped by cantonal police officers.

[3] The FIS may require the person stopped to provide their personal details and produce identity documents.

Art. 25 Special duties of private individuals to provide information

[1] Insofar as it is necessary to identify, prevent or repel a specific threat to internal or external security in accordance with Article 19 paragraph 2, the FIS may request the following information and records in specific cases:

a. from a natural person or legal entity that carries out transport operations for commercial gain or provides or arranges means of transport: information about a service that it has provided;

b. from private operators of security infrastructures, in particular image transmission and image recording devices: the handover of recordings, including recordings of events in public locations.

15 SR **173.32**

[2] The FIS may also obtain information in accordance with Article 15 of the Federal Act of 18 March 2016[16] on the Surveillance of Postal and Telecommunications Traffic (SPTA).[17]

Section 4 Information Gathering Measures requiring Authorisation

Art. 26 Forms of information gathering measures requiring authorisation

[1] The following information gathering measures require authorisation:

a.[18] surveillance of post and telecommunications and requests for marginal data relating to post and telecommunications in accordance with the SPTA[19];

a[bis].[20] the use of special technical devices to monitor telecommunications, to record transmissions or to identify a person or object or to ascertain their location if monitoring in accordance with letter a has been unsuccessful, would be without prospect of success or would be unreasonably difficult and the licences under telecommunications law for the special technical devices have been obtained;

b. the use of localisation devices to establish the location and the movements of persons or objects;

c. the use of monitoring devices in order to listen to and record words spoken in non-public places or to observe and record events at non-public or not generally accessible locations;

d. the intrusion into computer systems and computer networks in order to:

1. gather information available there or transmitted from there,
2. disrupt, prevent or slow down access to information where the computer systems and computer networks are being used for attacks on critical infrastructures;

e. the search of premises, vehicles or storage facilities in order to procure objects or information there or information transmitted from there.

[2] The measures shall be carried out covertly; the person concerned is not made aware thereof.

16 SR **780.1**
17 Amended by Art. 46 No 2 of the FA of 18 March 2016 on the Surveillance of Postal and Telecommunications Traffic, in force since 1 March 2018 (AS **2018** 117; BBl **2013** 2683).
18 Amended by Art. 46 No 2 of the FA of 18 March 2016 on the Surveillance of Postal and Telecommunications Traffic, in force since 1 March 2018 (AS **2018** 117; BBl **2013** 2683).
19 SR **780.1**
20 Inserted by Art. 46 No 2 of the FA of 18 March 2016 on the Surveillance of Postal and Telecommunications Traffic, in force since 1 March 2018 (AS **2018** 117; BBl **2013** 2683).

Art. 27 Principle

[1] The FIS may order an information gathering measure requiring authorisation if:

a. there is a specific threat in terms of Article 19 paragraph 2 letters a–d or the measure is required to safeguard other important national interests in accordance with Article 3;

b. the seriousness of the threat justifies the measure; and

c. intelligence investigations so far have been unsuccessful or would otherwise be without prospect of success or unreasonably difficult.

[2] The FIS shall obtain the authorisation of the Federal Administrative Court and clearance from the Head of the DDPS before carrying out the measure.

[3] If other federal and cantonal agencies are required to participate in carrying out the measure, the FIS shall issue them with a written order as soon as the authorisation of the Federal Administrative Court and clearance from the Head of the DDPS is granted. The information gathering measure must be kept secret.

Art. 28 Ordering information gathering measures requiring authorisation in relation to third parties

[1] The FIS may also order an information gathering measure requiring authorisation in relation to a third party if there is reason to believe that the person from whom it is intended to gather the information is using premises, vehicles or storage facilities belonging to the third party or the latter's postal addresses, telecommunication connection points, computer systems or computer networks in order to transmit, receive or store information.

[2] The measure may not be ordered if the third party belongs to one of the professional groups mentioned in Articles 171–173 CrimPC[21].

Art. 29 Authorisation procedure

[1] Where the FIS intends to order an information gathering measure requiring authorisation, it shall submit an application to the Federal Administrative Court with:

a. details of the specific objective of the information gathering measure and the reasons for its necessity and an explanation of why investigations have so far been unsuccessful, would be without prospect of success or would be unreasonably difficult;

b. details of the persons who will be affected by the information gathering measure;

c. a precise description of the information gathering measure and details of its statutory basis;

d. details of any other agencies that it is intended to instruct to carry out the information gathering measure;

21 SR **312.0**

e. details of when the information gathering measure will start and finish and the deadline by which it must be carried out;

f. the files required for granting authorisation.

2 The president of the competent division of the Federal Administrative Court shall issue as a single judge a decision with a brief statement of reasons within five working days of receipt of the application; he or she may delegate this task to another judge.

3 The president of the competent division of the Federal Administrative Court shall not authorise a requested information gathering measure if that measure has already been authorised in connection with criminal proceedings against the persons concerned in accordance with paragraph 1 letter b and the criminal investigation is connection with a specific threat that the FIS information gathering measure is intended to clarify. The competent courts responsible for compulsory measures or the Post and Telecommunications Surveillance Bureau shall provide the Federal Administrative Court with the required information.

4 The president of the competent division of the Federal Administrative Court may require a hearing of representatives of the FIS as part of the decision-making process.

5 He or she may grant authorisation subject to conditions or request further files or further investigations.

6 Authorisation applies for a maximum of three months. This period may be extended in any given case by a maximum of three months.

7 If an extension is required, the FIS shall file a substantiated application for an extension in accordance with paragraph 1 before the authorised period expires.

8 The president of the competent division of the Federal Administrative Court shall prepare an annual report for the attention of the Control Delegation (CDel).

Art. 30 Clearance

1 If the information gathering measure has been authorised, the Head of the DDPS, after consulting the Head of the FDFA and the Head of the Federal Justice and Police Department (FDJP) shall decide on clearance for the measure to be carried out. Cases of particular importance may be submitted to the Federal Council.

2 The consultation procedure must be conducted in writing.

Art. 31 Procedure in cases of urgency

1 In cases of urgency, the Director of the FIS may order the immediate use of information gathering measures requiring authorisation. He or she shall immediately inform the Federal Administrative Court and the Head of the DDPS. Either may terminate the information gathering measure with immediate effect.

2 The Director of the FIS shall file the application within 24 hours with the president of the competent division of the Federal Administrative Court and shall give reasons for the urgency.

3 The president of the competent division of the Federal Administrative Court shall notify the FIS of his or her decision within three working days.

4 If the information gathering measure has been authorised, the Head of the DDPS, after consulting the Head of the FDFA and the Head of the FDJP, shall decide on clearance for the measure to be continued.

Art. 32 Termination

1 The FIS shall terminate the information gathering measure requiring authorisation immediately, if:

a. the authorised period has expired;

b. the requirements for continuing with the measure are no longer fulfilled;

c. authorisation by the Federal Administrative Court or clearance from the Head of the DDPS is not granted.

2 In cases of urgency, the FIS shall ensure the immediate destruction of the data procured if:

a. the president of the competent division of the Federal Administrative Court rejects the application;

b. the Head of the DDPS terminates the information gathering measure with immediate effect or refuses clearance for continuation.

3 If other agencies are involved in carrying out the information gathering measure requiring authorisation, the FIS shall notify them of its termination.

4 The FIS shall notify the Federal Administrative Court and the Head of the DDPS of the termination of the information gathering measure.

Art. 33 Obligation to notify

1 The FIS shall notify the person being monitored within one month after conclusion of the operation of the reason for and nature and duration of monitoring using information gathering measures requiring authorisation.

2 It may postpone or dispense with giving notification if:

a. this is necessary so as not to jeopardise an ongoing information gathering measure or ongoing legal proceedings;

b. this is necessary due to another overriding public interest in order to safeguard internal or external security or Swiss foreign relations;

c. notification could cause serious danger to third parties;

d. the person concerned cannot be contacted.

3 Postponing or dispensing with notification must be authorised and cleared in accordance with Article 29.

Section 5 Cooperation and Protection of Sources

Art. 34 Cooperation and delegation of information gathering

1 The FIS may carry out the information gathering measures itself, work with domestic or foreign agencies, or delegate information gathering to such agencies provided the other agencies guarantee that information gathering will be carried out in accordance with this Act.

2 By way of exception, it may also work with private individuals or issue private individuals with assignments if this is required for technical reasons or to gain access to the object of information gathering and the person concerned offers a guarantee that information gathering will be carried out in accordance with this Act.

Art. 35 Protection of sources

1 The FIS shall ensure the protection of its sources and shall preserve their anonymity, in particular that of foreign intelligence services and security services and of persons who gather information about foreign countries and are endangered as a result. The foregoing does not apply to persons who are accused in criminal proceedings of serious crimes against humanity or war crimes.

2 The FIS shall disclose the identity of a human source resident in Switzerland to the Swiss prosecution authorities if the person concerned is suspected of an offence that is prosecuted ex officio or if disclosure is essential in order to identify the perpetrator of a serious offence.

3 The following must be considered in relation to the protection of sources:

a. the interests of the FIS in continuing to use the source for intelligence;

b. the need for human sources in particular to be protected from third parties;

c. in the case of technical sources: information that should be kept secret about infrastructure, performance capabilities, operational methods and procedures for procuring information.

4 In the event of a dispute, the Federal Criminal Court shall decide; the relevant provisions on mutual assistance also apply.

Section 6 Information Gathering about Events outside Switzerland

Art. 36 General provisions

1 The FIS may covertly gather information about events outside Switzerland.

2 Where the FIS procures information in Switzerland about events outside Switzerland, it is bound by the provisions of Section 4; Article 37 paragraph 2 remains reserved.

3 The FIS shall ensure that the risk in information gathering is not disproportionate to the expected benefit of information gathering and that interference with the fundamental rights of the persons concerned can be limited to what is necessary.

4 It shall document information gathering about events outside Switzerland for the attention of the supervision and control bodies.

5 It may store data separately from information gathering measures abroad that are comparable with information gathering measures requiring authorisation if this is required because of the volume of data, confidentiality or security.

6 FIS employees deployed abroad shall be insured during their mission under the Federal Act of 19 June 1992[22] on Military Insurance against Illness and Accident.

7 The FIS shall ensure the protection of its employees deployed abroad.

Art. 37 Intrusion into computer systems and computer networks

1 Where computer systems and computer networks located abroad are used to carry out attacks on critical infrastructures in Switzerland, the FIS may intrude into these computer systems and computer networks in order to disrupt, prevent or slow down access to information. The Federal Council shall decide on whether such a measure should be carried out.

2 The FIS may intrude into computer systems and computer networks abroad in order to gather information about events outside Switzerland that is available there or that has been transmitted from there. The Head of the DDPS shall decide after consulting the Head of the FDFA and the Head of the FDJP on whether such a measure should be carried out.

Art. 38 Radio communications intelligence

1 The Confederation may operate a service for recording electro-magnetic emissions from telecommunications systems located abroad (radio communications intelligence).

2 Radio communications intelligence has the following purposes:

a. information gathering about events outside Switzerland that are of significance to security, in particular relating to terrorism, the proliferation of weapons of mass destruction and foreign conflicts that have an effect on Switzerland;

b. safeguarding of other important national interests in accordance with Article 3.

3 The Federal Council shall regulate the fields of communications intelligence, and the organisation and procedures for radio communications intelligence. It shall specify for how long the recorded communications and connection data may be retained by the service carrying out the communications intelligence.

22 SR **833.1**

4 It shall in particular ensure that from the recorded communications the service carrying out the communications intelligence:

a. only passes on information relating to events outside Switzerland that are of significance to security;

b. only passes on information about persons in Switzerland if the information is required to understand an event abroad and has been anonymised beforehand.

5 The service carrying out the communications intelligence shall pass on information about events in Switzerland obtained from the recorded communications if the information provides evidence of a specific threat to internal security in accordance with Article 6 paragraph 1 letter a.

6 If it comes across recorded communications in the course of its activities that contain no information about events outside Switzerland that are of significance to security and no evidence of any specific threat to internal security, it shall destroy the recordings as quickly as possible.

Section 7 Cable Communications Intelligence

Art. 39 General Provisions

1 In order to gather information about events outside Switzerland that are of significance to security (Art. 6 para. 1 let. b) and to safeguard additional important national interests in accordance with Article 3, the FIS may instruct the service carrying out the communications intelligence to record cross-border signals from cable-based networks.

2 If both the transmitter and the recipient are located in Switzerland, the recorded signals in accordance with paragraph 1 may not be used. If the service carrying out communications intelligence cannot separate such signals during the recording process, the data procured shall be destroyed as soon as it is established that it originates from such signals.

3 Data from recorded signals may only be passed on to the FIS if its content corresponds to the search parameters defined for the operation. The search parameters must be defined so that their application causes as little interference as possible in the private domain of persons. Details of Swiss natural persons or legal entities are not permitted as search parameters.

4 The Federal Council shall regulate:

a. the permitted fields of communications intelligence;

b. the organisation and the details of the procedure for cable communications intelligence;

c. the maximum period that the service carrying out the communications intelligence may retain recorded content and connection data obtained from cable communications intelligence.

Art. 40 Authorisation requirement

[1] Cable communications intelligence mandates require authorisation.

[2] Before the FIS issues a mandate for cable communications intelligence it shall obtain the authorisation of the Federal Administrative Court and clearance from the Head of the DDPS.

[3] The Head of the DDPS shall consult the Head of the FDFA and the Head of the FDJP beforehand.

Art. 41 Authorisation procedure

[1] If the FIS intends to issue a mandate for cable communications intelligence, it shall file an application with Federal Administrative Court that includes:

a. a description of the mandate to be issued to the service carrying out the communications intelligence;

b. the reasons why the operation is necessary;

c. details of the categories of search parameters;

d. details of the operators of cable-based networks and the providers of telecommunications services that must supply the signals required to conduct the cable communications intelligence; and

e. details of when the operation will start and finish.

[2] The further procedure is governed by Articles 29–32.

[3] Authorisation applies for a maximum of six months. This period may be extended for a maximum of three months in any given case in accordance with the same procedure.

Art. 42 Conduct

[1] The service carrying out communications intelligence receives the signals from the operators and providers in accordance with Article 41 paragraph 1 letter d, converts them into data and assesses on the basis of the content which data is passed on to the FIS.

[2] It shall only pass on data to the FIS that contains information within the search parameters defined for fulfilment of the mandate. It shall only pass on information about persons in Switzerland to the FIS if the information is required to understand an event abroad and has been anonymised beforehand.

[3] If the data contains information about events in Switzerland or abroad that provides evidence of a specific threat to internal security in accordance with Article 6 paragraph 1 letter a, the service carrying out communications intelligence shall pass on the data unchanged to the FIS.

[4] The service carrying out communications intelligence must destroy data that does not contain any information in accordance with paragraphs 2 and 3 as quickly as possible.

5 The FIS is responsible for the intelligence evaluation of the data.

Art. 43 Obligations of operators of cable-based networks and providers of telecommunications services

1 Operators of cable-based networks and providers of telecommunications services are obliged to provide the service carrying out communications intelligence or the FIS with the technical information required to carry out the cable communications intelligence.

2 If clearance has been given for an operation, operators of cable-based networks and providers of telecommunications services are obliged to supply signals to the service carrying out communications intelligence. They must remove any encryption that they have applied.

3 Operators of cable-based networks and providers of telecommunications services are obliged to preserve secrecy about operations.

4 The Confederation shall compensate operators of cable-based networks and providers of telecommunications services. The Federal Council shall regulate the level of compensation based on the cost of supplying the signals to the service carrying out communications intelligence.

Chapter 4 Data Processing and Archiving

Section 1 Principles, Quality Assurance and Data Processing in the Cantons

Art. 44 Principles

1 The FIS and the cantonal executive authorities are authorised to process personal data, including personal data that permits an assessment of the level of risk that a person poses, irrespective of whether the data are sensitive personal data or not.[23]

2 The FIS may also process information that proves to be disinformation or false information if this is necessary in order to assess the situation or a source. It shall mark the relevant data as incorrect.

3 It may transfer the same data to several information systems. The specifications for the information system concerned apply.

4 It may record data within an information system through a network and evaluate it automatically.

23 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

Art. 45 Quality assurance

[1] The FIS shall assess the relevance and accuracy of personal data before recording it in an information system. Reports that contain several sets of personal data shall be assessed in their entirety before they are recorded in the filing system.

[2] It shall only record data that may be used to fulfil the tasks in accordance with Article 6, subject to compliance with Article 5 paragraphs 5–8.

[3] It shall destroy data that may not be recorded in any information system or return it to the sender for further investigation or for processing on the sender's own initiative.

[4] It shall periodically check in all information systems whether the recorded sets of personal data are still required to carry out its tasks. It shall delete data records that are no longer required. Incorrect data shall be corrected immediately or deleted; Article 44 paragraph 2 remains reserved.

[5] The FIS's internal quality assurance service shall carry out the following tasks:

a. it shall review the personal data in the system IASA-GEX FIS (Art. 50) with regard to its relevance and accuracy;

b. it shall periodically review the reports from the cantonal executive authorities recorded in the INDEX FIS system (Art. 51) with regard to their relevance and accuracy;

c. it shall verify by random sample the legality, expediency, effectiveness and accuracy of the data processing in all FIS information systems;

d. it shall delete data in the INDEX FIS system that originates from preliminary investigations conducted by the cantons which was recorded more than five years previously, and data whose deletion is requested by the canton;

e. it shall arrange internal training sessions for FIS employees on data protection matters.

Art. 46 Data processing in the cantons

[1] The cantonal executive authorities shall not maintain any databases of their own in application of this Act.[24]

[2] If the cantons process data on their own initiative, they shall ensure that the cantonal data makes no reference to the existence or content of federal data.

[3] The cantonal executive authorities may pass on situation assessments and data that they receive from the FIS if this is necessary in order to assess measures to safeguard security or to avert a significant danger. The Federal Council shall regulate the agencies and the extent to which assessments and data may be passed on.

24 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

Section 2 Intelligence Information Systems

Art. 47 FIS information systems

[1] The FIS shall operate the following information systems in order to carry out its tasks in accordance with Article 6:

a. IASA FIS (Art. 49);
b. IASA-GEX FIS (Art. 50);
c. INDEX FIS (Art. 51);
d. GEVER FIS (Art. 52);
e. ESD (Art. 53);
f. OSINT portal (Art. 54);
g. Quattro P (Art. 55);
h. ISCO (Art. 56);
i. residual data memory (Art. 57).

[2] For each FIS information system, the Federal Council shall regulate:

a. the catalogue of personal data;
b. responsibilities for data processing;
c. access rights;
d. the frequency of quality assurance, taking account of the seriousness of the interference in constitutional rights caused by data processing;
e. the retention period for the data, taking account of the specific needs of the FIS in relation to the task areas concerned;
f. the deletion of the data;
g. data security.

Art. 48 Allocation of data to the information systems

The FIS shall allocate incoming data as follows:

a. data with information about violent extremism: to the IASA-GEX FIS system;
b. data with information that initiates administrative processes only: the GEVER FIS system;
c. data with information related to security measures only: the ESD system;
d. data from publicly accessible sources: the OSINT portal system;
e. data from border and customs checks: the Quattro P system;
f. data that is used only for task management and for controlling radio and cable communications intelligence: the ISCO system;
g. other data: the residual data memory system.

Art. 49 IASA FIS

[1] The FIS integral analysis system (IASA FIS) is used for the intelligence evaluation of data.

[2] It contains data relating to the task areas in Article 6 paragraph 1, with the exception of data on violent extremism.

[3] FIS employees that have the task of recording, researching, evaluating and assuring the quality of the data have online access to IASA FIS. They may carry out data searches with the aid of IASA FIS in all FIS information systems to which they hold access rights.

Art. 50 IASA-GEX FIS

[1] The FIS integral analysis system for violent extremism (IASA-GEX FIS) is used for recording, processing and evaluating information relating to violent extremism.

[2] It contains data relating to violent extremism.

[3] FIS employees that have the task of recording, researching, evaluating and assuring the quality of the data have online access to IASA-GEX FIS.

Art. 51 INDEX FIS

[1] The INDEX FIS information system is used:

a. to establish whether the FIS is processing data relating to a person, an organisation, a group, an object or an event;

b. to store reports prepared by the cantonal executive authorities;

c. to process data from preliminary investigations carried out by the cantonal executive authorities.

[2] It enables authorities that are not connected to the specially secured FIS network to access data that they need to fulfil their statutory tasks, and the secure transmission of such data.

[3] It contains:

a. data for the identification of the persons, organisations, groups, objects and events recorded in the IASA FIS and IASA-GEX FIS information systems;

b. the reports prepared by the cantonal executive authorities independently or on behalf of the FIS;

c. data from preliminary investigations carried out by the cantonal executive authorities.

[4] The following persons have online access to the following data in INDEX FIS:

a. FIS employees have access to the data in paragraph 3 letters a and b, provided they have the task of ensuring the early recognition and prevention of threats to Switzerland and its population;

b. employees of the cantonal executive authorities in order to carry out their tasks in terms of this Act and to process and pass on their data from preliminary investigations and their reports to the FIS and to other cantonal executive authorities; only employees of the cantonal executive authority that carried out the preliminary investigations and the employees of the FIS quality assurance service have access to data in accordance with paragraph 3 letter c;

c. employees of the Federal Office of Police have access to the data in accordance with paragraph 3 letter a in order to conduct security-related, criminal investigation and administrative-policing tasks and to assess allegations of money laundering and terrorism financing contained in reports from Swiss financial institutions;

d.[25] the employees of the specialist units in accordance with Article 31 paragraph 2 of the Information Security Act of 18 December 2020[26] responsible for carrying out personnel security screening procedures have access to the data in accordance with paragraph 3 letter a in order to carry out personnel security screening procedures and assess trustworthiness and potential for violence.

Art. 52 GEVER FIS

[1] The FIS information system for records and process management (GEVER FIS) is used for the processing and control of business and to ensure efficient work processes.

[2] It contains:

a. data on administrative transactions;

b. all outgoing FIS intelligence products;

c. data that was used to prepare content in terms of letters a and b;

d. information required for the business controls, in particular in connection with personnel security screening procedures.

[3] FIS employees have online access to GEVER FIS.

Art. 53 ESD

[1] The Electronic Situation Display system (ESD) is used by the competent federal authorities and the cantons as a management instrument and for disseminating information with a view to controlling and implementing security policy measures, in particular in the event of incidents in which acts of violence are anticipated.

[2] It contains data about incidents and about measures to safeguard internal or external security.

[3] FIS employees and the responsible federal and cantonal authorities that have the task of managing security policy or assessing or dealing with situation-relevant incidents have online access to the ESD.

25 Amended by Annex 1 No 2 of the Information Security Act of 18 Dec. 2020, in force since 1 Jan. 2024 (AS **2022** 232; **2023** 650; BBl **2017** 2953).
26 SR **128**

4 In the case of special incidents, the FIS may also allow private agencies and foreign security and police authorities temporary online access. Access is limited to the data in the system that these agencies and authorities require to fulfil their tasks in dealing with the incident concerned.

Art. 54 OSINT portal

1 The FIS uses the Open Source Intelligence Portal (OSINT portal) to obtain data from publicly accessible sources.

2 It contains data that is available when using publicly accessible sources.

3 FIS employees have online access to the OSINT portal.

4 Employees of the cantonal executive authorities may be allowed online access to certain data in the OSINT portal.

Art. 55 Quattro P

1 The FIS may operate an information system (Quattro P) that is used to identify certain categories of foreign nationals that enter or leave Switzerland and to monitor their entry and exit data.

2 It contains data obtained at border posts in the course of border and customs checks which may be used to identify the persons and track their travel movements.

3 FIS employees that are required to identify persons in order to fulfil tasks in accordance with Article 6 have online access to Quattro P.

4 The Federal Council shall determine in a non-public list the categories of persons to be recorded in Quattro P; in doing so it shall take account of the threat situation at the time.

Art. 56 ISCO

1 The communications monitoring information system (ISCO) is used to monitor and direct radio and cable communications intelligence.

2 It contains data to operate the intelligence gathering equipment and for controlling and reporting.

3 FIS employees that have the task of carrying out radio and cable communications intelligence have online access to ISCO.

Art. 57 Residual data memory

1 The residual data memory is used to store data that cannot be immediately allocated to another system in accordance with Article 48.

2 If an information entry in the residual data memory contains personal data, an assessment of relevance and accuracy in accordance with Article 45 paragraph 1 is made for the entry as a whole and not in relation to the individual personal data. An individual assessment is made if the personal data is transferred to another information system.

3 FIS employees that have the task of recording, researching, evaluating and assuring the quality of the data have online access to the residual data memory.

4 The maximum retention period for the data is 10 years.

Section 3
Data from Information Gathering Measures requiring Authorisation

Art. 58

1 The FIS shall store the data from information gathering measures requiring authorisation in accordance with Article 26 on a case-related basis and separately from the information systems listed in Article 47.

2 It shall ensure that personal data originating from information gathering measures requiring authorisation that is not related to the specific threat situation is not used and is destroyed at the latest 30 days after conclusion of the measure.

3 If the information gathering measure requiring authorisation relates to a person who belongs to any of professional groups mentioned in Articles 171–173 CrimPC[27], data that is not related to the specific threat situation shall be separated and destroyed under the supervision[28] of the Federal Administrative Court. If the information gathering measure requiring authorisation relates to another person, data about which a person has the right to refuse to testify in accordance with Articles 171–173 CrimPC must also be destroyed.

4 In specific cases and subject to compliance with Article 5 paragraphs 5–8, it may also store personal data in the information system provided for this purpose in accordance with Article 47 paragraph 1, provided it contains information required to fulfil tasks in accordance with Article 6 paragraph 1.

5 FIS employees that have the task of carrying out a information gathering measure and evaluating the results have online access to the relevant data.

6 The Federal Council shall regulate:

a. the catalogue of personal data;

b. the processing and access rights;

c. the retention period for the data and the procedure for destroying data;

d. data security.

27 SR **312.0**
28 Corrected by the Federal Assembly Drafting Committee (Art. 58 para. 1 ParlA; SR **171.10**).

Section 4 Special Provisions on Data Protection

Art. 59 Verification before disclosure

The FIS shall ensure before disclosing any personal data or products that the personal data satisfies the legal requirements of this Act and that its disclosure is lawful and necessary in the case concerned.

Art. 60 Disclosure of personal data to Swiss authorities

1 The FIS shall disclose personal data to domestic authorities if this is necessary in order to safeguard internal or external security. The Federal Council shall determine the authorities concerned.

2 Where information obtained by the FIS may be used by other authorities to prosecute offences, prevent serious offences or to maintain public order, the FIS shall while protecting its sources make this data available to them without being requested to do so or on request.

3 The FIS shall always disclose data from information gathering measures requiring authorisation to a prosecution authority if it contains specific evidence of an offence in connection with the prosecution of which the prosecution authority would have been entitled to order a comparable criminal procedural measure.

4 The FIS shall advise the prosecution authorities of the origin of the data. The subsequent procedure is governed by the CrimPC[29] or the Military Criminal Procedure Code of 23 March 1979[30].

Art. 61 Disclosure of personal data to foreign authorities

1 The FIS may disclose personal data or lists of personal data to foreign countries. It shall verify before any disclosure whether the legal requirements for disclosure are met.

2 If the legislation of the receiving state does not guarantee appropriate data protection, the personal data may be disclosed to this state in derogation from Article 16 paragraph 1 of the Data Protection Act of 25 September 2020[31] on (FADP) only if Switzerland maintains diplomatic relations with that state and one of the following requirements is met:[32]

a. Switzerland is required by law or by an international agreement to disclose the personal data to the state.

b. Disclosure is required to safeguard an overriding public security interest in Switzerland or in the receiving state such as preventing a serious criminal

29 SR **312.0**
30 SR **322.1**
31 SR **235.1**
32 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

offence which is also a serious offence in Switzerland or bringing its perpetrators to justice.

c. It is necessary in order to justify a request for information from Switzerland.

d. It is in the interest of the person concerned and this person has already consented to disclosure or his or her consent may be clearly assumed in the circumstances.

e. It is necessary in order to protect the life and limb of third parties.

3 The FIS may in specific cases disclose personal data to states with which Switzerland maintains diplomatic relations if the requesting state provides a written assurance that it has the consent of the person concerned, and the requesting state will as a result be able to assess whether the person concerned can participate in classified projects carried out by that foreign state in relation to internal or external security or have access to classified information, materials or facilities of that foreign state.

4 It may disclose personal data online to foreign security agencies whose states guarantee an appropriate standard of data protection and with which Switzerland has concluded an agreement in accordance with Article 70 paragraph 3.

5 Personal data may not be disclosed to a foreign security agency if the person concerned will be exposed to the risk of being punished twice or of serious harm to his or her life, limb or freedom in terms of the Convention of 4 November 1950[33] on the Protection of Human Rights and Fundamental Freedoms or other international agreements that Switzerland has ratified.

6 If the personal data is required in legal proceedings, the relevant provisions on mutual assistance apply.

Art. 62 Disclosure of personal data to third parties

The disclosure of personal data to third parties is only permitted if:

a. the person concerned has consented to disclosure or disclosure is indisputably in the interest of the person concerned;

b. disclosure is necessary in order to repel a serious immediate danger;

c. disclosure is necessary in order to justify a request for information.

Art. 63 Right to information

1 The right to information relating to the ESD, OSINT portal and Quattro P information systems, the administrative data in GEVER FIS and data in the storage systems in accordance with Articles 36 paragraph 5 and 58 is governed by the FADP[34].

2 If a person requests information on whether the FIS is processing data on them in the IASA FIS, IASA-GEX FIS, INDEX FIS or ISCO information systems, the residual data memory or in the GEVER FIS intelligence data, the FIS shall defer its response:

33 SR **0.101**
34 SR **235.1**

a. if and to the extent that there are overriding interests that are justified in the files in preserving secrecy in relation to the data about the person that is being processed that are connected with:
   1. the fulfilment of a task in accordance with Article 6, or
   2. a prosecution or other investigation;
b. if and to the extent that it is required because of overriding interests of third parties; or
c. if no data about the applicant is being processed.

3 The FIS shall notify the applicant that it is deferring the provision of information and advise the applicant that they have the right to request the Federal Data Protection and Information Commissioner (FDPIC) that he examine whether the data, if any, is being lawfully processed and whether overriding interests in preserving secrecy justify the deferral.

4 As soon as there are no longer any interests in preserving secrecy, but at the latest on expiry of the retention period, the FIS shall provide the applicant with information in accordance with the FADP unless there is excessive work and expense involved.

5 The FIS shall notify persons in respect of whom no data is being processed of this fact no later than three years after receipt of their request.

Art. 64 Examination by the FDPIC

1 The FDPIC shall conduct an examination in accordance with Article 63 paragraph 3 if so requested by the applicant.

2 It shall notify the applicant either that no data relating to the applicant has been unlawfully processed or that it has identified errors relating to the deferral of the provision of information and has opened an investigation under Article 49 FADP[35].[36]

3 …[37]

4 If it identifies errors while processing the data or when deferring the provision of information, it shall order the FIS to rectify the same.[38]

5 If the applicant credibly shows that a deferral of the provision of information will cause him or her considerable harm that cannot be rectified, the FDPIC may order the FIS to issue information immediately by way of exception provided this will not pose a risk to internal or external security.[39]

35 SR **235.1**
36 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).
37 Repealed by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, with effect from 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).
38 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).
39 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

Art. 65[40]

Art. 66 Form of notification and exclusion of appeals

[1] The notifications in accordance with Articles 63 paragraph 3 and 64 paragraph 2 shall always be worded in the same way and do not contain a statement of reasons.[41]

[2] The persons concerned may not contest the notifications.

Art. 67 Exception from the principle of freedom of information

The Freedom of Information Act of 17 December 2004[42] does not apply to access to official documents relating to information gathering in terms of this Act.

Section 5 Archiving

Art. 68

[1] The FIS shall offer data and files that are no longer required or that are earmarked for destruction to the Federal Archives. The Federal Archives shall archive data and files from the FIS in specially secured rooms. They are subject to a 50-year retention period.

[2] For archive materials that originate from foreign security services, the Federal Council may extend the retention period on several occasions for a limited period in accordance with Article 12 of the Archiving Act of 26 June 1998[43] if the foreign security service concerned expresses reservations against any inspection.

[3] The FIS may in specific cases inspect personal data during the retention period that it has passed to the Federal Archives for archiving in order to assess specific threats to internal or external security or to safeguard any other overriding public interest.

[4] It shall destroy data and files that the Federal Archives has designated as not worth archiving.

Chapter 5 Services

Art. 69

[1] Where there is an intelligence interest or other public interest, the FIS may provide services to other federal and cantonal authorities in the following areas in particular:

a. secure transmission;

40 Repealed by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, with effect from 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).
41 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).
42 SR **152.3**
43 SR **152.1**

b. transport of goods or persons;

c. advice and situation assessment;

d. protection and defence against attacks on the information or communications infrastructure or on secrecy.

2 Where there is an intelligence interest, the FIS may also provide the foregoing services to third parties in Switzerland or abroad.

Chapter 6 Political Governance, Control and Legal Remedies

Section 1 Political governance and Bans

Art. 70 Political governance by the Federal Council

1 The Federal Council shall exercise political governance over the FIS and carry out the following tasks in particular for that purpose:

a. It shall issue the FIS with a basic mission and renew this mission at least every four years; the basic mission shall remain secret.

b. It shall authorise the watch list in accordance with Article 72 every year and submit it to the CDel; the watch list is confidential.

c. It shall determine the groups every year that must be categorised as violent-extremist groups and shall take note of the number of violent extremists that cannot be assigned to any known group.

d. It shall assess the threat situation every year and as required in the event of incidents and shall inform the Federal Assembly and the general public.

e. It shall order the required measures in the case of special threat situations.

f. It shall decide every year on how the FIS will cooperate with foreign authorities.

2 The documents in connection with the tasks in paragraph 1 shall not be made accessible to the public.

3 The Federal Council may on its own initiative conclude international agreements on the international cooperation of the FIS in relation to the protection of information or participation in international automated information systems in accordance with Article 12 paragraph 1 letter e.

Art. 71 Safeguarding other important national interests

1 In the event of a serious and immediate threat, the Federal Council may instruct the FIS to carry out measures in terms of this Act to the extent that these measures are required to safeguard other important national interests in accordance with Article 3.

2 It shall in each case determine the duration, purpose, nature and extent of the measure.

3 In the case of information gathering measures requiring authorisation, the authorisation procedure in accordance with Articles 26–33 must be complied with.

4 If the Federal Council issues instructions in accordance with paragraph 1, it shall inform the CDel within 24 hours.

Art. 72 Watch list

1 The watch list contains details of organisations and groups that are reasonably assumed to pose a threat to internal or external security.

2 The assumption is deemed to be reasonable where an organisation or group appears on a list kept by the United Nations or the European Union; in this case, this organisation or group may be included on the watch list.

3 An organisation or group shall be removed from the watch list if:

a. the assumption that it poses a threat to internal or external security no longer applies; or

b. it no longer appears on any list in accordance with paragraph 2 and there are no particular reasons why it should pose a threat to internal or external security.

4 The Federal Council shall set out in an ordinance the criteria by which the watch list is drawn up; it shall determine the periodicity for reviewing the list.

Art. 73 Order banning an activity

1 The Federal Council may ban a natural person or an organisation or group from carrying out an activity that poses a specific threat to internal or external security and directly or indirectly serves to propagate, support or otherwise promote terrorist or violent-extremist activities.

2 A ban may be imposed for a maximum of five years. If the requirements are still met on expiry of this period, the ban may be extended for a maximum of five further years.

3 The applicant department shall regularly review whether the requirements are still being met. If this is no longer the case, it shall apply to the Federal Council for the ban to be lifted.

Art. 74 Organisation ban

1 The Federal Council may ban an organisation or group that directly or indirectly propagates, supports or otherwise promotes terrorist or violent-extremist activities and thus poses a specific threat to internal or external security.

2 A ban shall be based on a United Nations resolution on a ban or on sanctions; the Federal Council shall consult the committees responsible for security policy.[44]

44 Amended by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).

3 A ban may be imposed for a maximum of five years. If the requirements are still met on expiry of this period, the ban may be extended for a maximum of five further years.

4 Any person who on Swiss territory participates in an organisation or group banned under paragraph 1, supports it by providing human or other resources, organises propaganda campaigns for its aims, recruits for it or in any other way promotes its activities shall, be liable to a custodial sentence not exceeding five years or to a monetary penalty.[45]

4bis The court may reduce the penalty in accordance with paragraph 4 (Art. 48*a* SCC[46]) if the offender makes an effort to foil the further activities of the organisation or group.[47]

5 It is an offence for any person to commit the foregoing offence outside Switzerland if that person is arrested in Switzerland and not extradited. Article 7 paragraphs 4 and 5 SCC[48] applies.

6 The prosecution and adjudication of acts under paragraphs 4 and 5 are subject to federal jurisdiction.[49]

7 The responsible authorities shall notify the FIS of any judgments, penalty orders and decisions to dismiss proceedings immediately and free of charge, providing copies of all related documents.[50]

Section 2 Control and Supervision of the FIS

Art. 75 Self-control by the FIS

The FIS shall ensure by means of suitable quality assurance and control measures that the lawful implementation of this Act both within the FIS and within the cantonal security services is guaranteed.

45 Amended by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).
46 SR **311.0**
47 Inserted by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).
48 SR **311.0**
49 Amended by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).
50 Amended by Annex No II 1 of the FA of 25 Sept. 2020 on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, in force since 1 July 2021 (AS **2021** 360; BBl **2018** 6427).

Art. 76 Independent supervisory authority

[1] The Federal Council shall establish an independent authority to oversee the FIS.

[2] In response to a proposal from the DDPS, it shall appoint the director of the independent supervisory authority for a term of six years.

[3] The director shall be re-appointed for a further term unless the Federal Council rules at the latest six months before the end of the current term that this is not appropriate on objectively reasonable grounds.

[4] The director may resign from the post as of the end of any month subject to giving six months' notice thereof to the Federal Council.

[5] He or she may be removed from the post by the Federal Council before the expiry of the term office if he or she:

a. breaches his or her official duties wilfully or through gross negligence; or

b. becomes permanently incapable of exercising office.

Art. 77 Status of the independent supervisory authority

[1] The independent supervisory authority shall carry out its tasks independently; it is not bound by directives from other authorities. It is assigned to the DDPS for administrative purposes.

[2] It has its own budget. It appoints its own staff.

[3] It constitutes itself. It shall regulate its organisation and its working methods in its own procedural rules.

[4] The employment contracts of the head and the staff of the independent supervisory authority are governed by the Federal Personnel Act of 24 March 2000[51]. The head is not subject to the assessment system in accordance with Article 4 paragraph 3 of the Federal Personnel Act.[52]

Art. 78 Tasks, rights to information and recommendations of the supervisory authority

[1] The independent supervisory authority shall oversee the intelligence service activities carried out by the FIS, cantonal executive authorities and third parties and other agencies delegated these tasks by FIS. It shall audit these activities to confirm their legality, expediency and effectiveness.

[2] It shall coordinate its activities with parliamentary supervision activities and with other federal and cantonal supervision bodies.

[3] It shall inform the DDPS about its activities in an annual report; this report shall be published.

51 SR **172.220.1**

52 The correction of the FA Drafting Committee of 12 March 2020, published 24 March 2020, relates to the French text only (AS **2020** 1057).

4 It has access to all relevant information and documents and access to all the premises of the subjects of supervision. It may request copies of documents. Within the scope of its supervision activities, it may request information from and may inspect files held by other federal and cantonal agencies, provided this information is related to the cooperation between these agencies and the subjects of supervision.

5 In order to carry out its supervision activities, it may have access to all the information systems and databases of the subjects of supervision; it may also have access to sensitive personal data. It may only store the data thereby obtained until the audit is completed. The controllers concerned must keep a record of access to the various information systems and databases.[53]

6 The independent supervisory authority shall provide the DDPS with a written report on the results of its audit. It may issue recommendations.

7 The DDPS shall ensure that the recommendations are implemented. If the DDPS rejects a recommendation, it shall submit the same to the Federal Council for a decision.

Art. 79 Independent control authority for radio and cable communications intelligence

1 An independent control authority within the Administration shall verify the legality of radio communications intelligence and supervise the conduct of authorised and cleared cable communications intelligence assignments. In carrying out its tasks, it is not bound by directives from other authorities. The Federal Council shall appoint its members.

2 The control authority shall examine the assignments given to the service carrying out communications intelligence and the processing and passing on of information that this service has obtained. For this purpose, it shall be granted access by the responsible agencies to all relevant information and facilities.

3 It may issue recommendations based on its audit and request that the DDPS terminate radio communications intelligence assignments and delete information. Its recommendations, requests and reports are not made public.

4 The Federal Council shall regulate the composition and the organisation of the control authority, the remuneration of its members and the organisation of its Secretariat. The term of office amounts to four years.

Art. 80 Supervision and control by the Federal Council

1 The DDPS shall inform the Federal Council regularly about the threat situation and the activities of the FIS.

2 The Federal Council shall regulate:

a. financial supervision over the spheres of activity of the FIS that require particular confidentiality;

53 Amended by Annex 1 No II 2 of the Data Protection Act of 25 Sept. 2020, in force since 1 Sept. 2023 (AS **2022** 491; BBl **2017** 6941).

b. the minimum requirements for control in the cantons and the responsibilities of federal supervision bodies.

3 International administrative agreements concluded by the FIS that are of long-term duration, have substantial financial consequences or of which the Federal Council should be notified for legal or political reasons require approval by the Federal Council. This requirement of approval also applies to unwritten agreements. The agreements may only be implemented once approval is given.

4 The DDPS shall inform the Federal Council and the CDel annually or as required about the purpose and number of alias identities being used by employees of the FIS or cantonal security agencies. The number of newly issued identity documents must be shown separately.

5 The Federal Council shall inform the CDel annually and as required about bans on activities and the results of the regular review in accordance with Article 73 paragraph 3 and about bans of organisations.

Art. 81 Parliamentary oversight

1 Parliamentary oversight of the activities of the FIS and the cantonal executive authorities acting on behalf of the Confederation in implementing this Act is the responsibility in their respective spheres of the CDel and the Finance Delegation in accordance with the Parliament Act of 13 December 2002[54].

2 Cantonal parliamentary supervisory bodies may oversee implementation in accordance with Article 85 paragraph 1.

Art. 82 Cantonal supervision

1 Employees of the cantonal executive authorities that are entrusted by the cantons with tasks in terms of this Act are governed by cantonal public service legislation and subject to the cantonal supervision of their superiors.

2 Supervision in the cantons is the responsibility of the superior authorities to the cantonal executive authority concerned. These authorities may employ a control authority in order to provide assistance with supervision; this body must be separate from the cantonal executive authority and accountable to the superior authorities.

3 In order to exercise its supervisory activities, the cantonal supervisory authority shall be provided with a list of assignments issued by the FIS and the watch list in accordance with Article 72.

4 The cantonal supervisory authority may inspect the data that the canton is processing on behalf of the Confederation. Inspection may be refused if essential security interests so require.

5 The Federal Council shall regulate the inspection procedure. In the case of disputes, an action may be brought in the Federal Supreme Court in accordance with Article 120 paragraph 1 letter b of the Federal Supreme Court Act of 17 June 2005[55].

54 SR **171.10**
55 SR **173.110**

6 The Federal Council shall regulate the support given to the cantonal supervisory authority by federal agencies.

Section 3 Legal Remedies

Art. 83

1 Rulings based on this Act issued by federal bodies may be contested by appeal to the Federal Administrative Court.

2 An appeal against a ruling on the special obligation imposed on private individuals to provide information and on a ban on activities or organisations does not have the effect of suspending the ruling.

3 The period allowed for filing the appeal against an order for an information gathering measure requiring authorisation begins on the day that notice of the measure is received.

4 Appeal decisions of the Federal Administrative Court may be appealed to the Federal Supreme Court. The procedure is governed by the Federal Supreme Court Act of 17 June 2005[56].

Chapter 7 Final Provisions

Art. 84 Implementing provisions

The Federal Council shall issue the implementing provisions.

Art. 85 Implementation by the cantons

1 The cantons shall gather and process information in accordance with Article 6 paragraph 1 letter a without having to be requested to do so or based on a special assignment issued by the FIS. When doing so, the cantonal executive authorities have the power to make use on their own initiative of information gathering measures not requiring authorisation in accordance with Articles 13–15, 19, 20, 23 and 25.

2 The cantonal executive authorities shall submit a report to the FIS without having to be requested to do so if they identify a specific threat to internal or external security.

3 The FIS shall work with the cantons to implement this Act, in particular by providing technical resources, through protective and monitoring measures and by offering joint training courses.

4 The cantons shall within the limits of their capacities support the FIS in implementing its tasks, in particular by:

a. providing the required technical resources;

56 SR **173.110**

b. organising the required protective and observation measures;

c. assisting with training.

5 The Confederation shall within the limits of the approved credits compensate the cantons for their support in implementing this Act. The Federal Council shall fix the level of compensation based on the number of persons primarily employed to carry out federal tasks.

Art. 86 Repeal and amendment of other enactments

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

Art. 87 Coordination with the Amendment of 25 September 2015 of the Civilian Service Act

…[57]

Art. 88 Referendum and commencement

1 This Act is subject to an optional referendum.

2 The Federal Council shall determine the commencement date.

Commencement date: 1 September 2017[58]

57 The coordination provision may be consulted under AS **2017** 4095.
58 FCD of 16 Aug. 2017.

Annex
(Art. 86)

Repeal and amendment of other legislation

I

The Federal Act of 3 October 2008[59] on Responsibilities in the Area of the Civilian Intelligence Service is repealed.

II

The legislation below is amended as follows:

...[60]

59 [AS **2009** 6565, **2012** 3745 Annex No 1 5525, **2014** 3223]
60 The amendments may be consulted under AS **2017** 4095.