U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General *Washington, D.C. 20530*

Memorandum in Support of Designation of Switzerland as a Qualifying State Under Executive Order 14086

Executive Order 14086, signed on October 7, 2022, establishes a two-level redress mechanism for the review of qualifying complaints filed by individuals through an appropriate public authority in a "qualifying state" and alleging certain violations of U.S. law concerning signals intelligence activities. The Attorney General may designate a country or a "regional economic integration organization" as a qualifying state if he determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that it meets three requirements set forth in section 3(f) of the Executive Order.

This memorandum, prepared by the National Security Division of the Department of Justice, provides information in support of designating Switzerland as a qualifying state, by showing how Switzerland meets the three requirements in section 3(f) of Executive Order 14086. Designating Switzerland as a qualifying state, so that Swiss individuals may file complaints through the redress mechanism established by Executive Order 14086, is an essential step for Switzerland to recognize the adequacy of protection provided by the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF"). Switzerland's recognition of adequacy will in turn permit the transfer under Swiss law of personal information for commercial purposes in reliance on the Swiss-U.S. DPF from the territory of Switzerland to the territory of the United States.

I. Determinations to be made to designate a "qualifying state" under Executive Order 14086

Section 3(f) of Executive Order 14086 lists three determinations to be made to designate a country or regional economic integration organization a "qualifying state," followed by three corresponding determinations any one of which may be a basis to revoke or amend a designation:

> *(i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:*
>
> > *(A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for*

United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and

(C) such designation would advance the national interests of the United States.

(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or

(C) such designation is not in the national interests of the United States.

II. Determination that the laws of Switzerland require appropriate safeguards for signals intelligence activities affecting U.S. persons

The first determination to be made to designate Switzerland, pursuant to section 3(f)(i)(A) of Executive Order 14086, is that the laws of Switzerland "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of Switzerland. The following discussion describes how the laws of Switzerland meet this standard.

As a threshold matter, it is important to note that Executive Order 14086 does not require a "qualifying state" to provide identical or reciprocal safeguards to those provided under U.S. law. Rather, the Executive Order simply calls for a determination that the laws of the qualifying

state "require appropriate safeguards." The flexibility inherent in this standard accounts for the fact that different countries, even those sharing democratic values and a commitment to the rule of law, will have legal and national security systems with differing histories and institutions, such that they may legitimately take differing approaches towards enacting privacy safeguards for signals intelligence activities. In other words, the Executive Order's "appropriate safeguards" standard does not impose a rigid "one-size-fits-all" model, but rather asks, in light of the importance of maintaining trust and confidence in the free flow of data in today's networked global economy, whether the laws of a potential qualifying state, when viewed holistically, require appropriate privacy safeguards with respect to its national security activities.

The following discussion analyzes the privacy safeguards required by the laws of Switzerland in the conduct of signals intelligence activities that may affect U.S. persons' personal information that is transferred from the United States to Switzerland, including through Switzerland's ratification of and adherence to the European Convention on Human Rights. The discussion refers to the paper attached to this memorandum on privacy safeguards in Swiss law, in particular relating to signals intelligence activities, which the Swiss government has provided "in support of Switzerland's designation by the Attorney General of the United States as a 'qualifying state' pursuant to section 3(f) of Executive Order 14086" (the "Swiss Paper").

The analysis below demonstrates that the laws of Switzerland require comprehensive and detailed safeguards for signals intelligence activities that may affect U.S. persons' personal information that is transferred from the United States to Switzerland. Safeguards in Swiss law include requirements for prior judicial approval for signals intelligence collection activities, either for individual targeting decisions or on a programmatic basis for foreign-focused non-individualized surveillance; requirements of proportionality of actions and use of least-privacy intrusive methods; restrictions on the handling of data acquired; proactive supervision of intelligence activities; and a path to redress for individual complainants before the Swiss data protection authority.

To be sure, there are areas of divergence between the laws of the United States and the laws of Switzerland. For example, in contrast to Section 702 of the Foreign Intelligence Surveillance Act in the United States, the Swiss authorization to conduct analogous foreign-focused surveillance within Switzerland of electronic communications passing into Swiss territory is not limited to acquiring the electronic communications of specific persons who are suspected of communicating information of foreign intelligence interest. Instead, electronic communications may be acquired under the Swiss program through filtering based on key words, resulting in bulk collection as that term is understood in U.S. law. However, the numerous safeguards embedded throughout the Swiss legal regime demonstrate Switzerland's clear commitment to the protection of privacy with respect to its signals intelligence activities. Safeguards in the Swiss legal regime relevant to its foreign-focused non-individualized collection program include querying limitations; documentation requirements; and proactive, independent oversight. In this connection, it is also notable that Switzerland and the United States have both signed the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which sets forth principles for protecting privacy during government access to data for law enforcement and national security purposes, describing the legal protections for privacy that both countries share in connection with these activities. In that

OECD Declaration, the United States affirms that it takes into account a destination country's effective implementation of the Declaration's principles as a positive contribution towards facilitating transborder data flows.

Based on the below analysis, as well as the deferential "appropriate safeguards" standard in Executive Order 14086, and the importance of commercial transfers of data between Switzerland and the United States, it is within the Attorney General's discretion to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that the laws of Switzerland require appropriate safeguards for purposes of a section 3(f)(i)(A) determination.

a. The European Convention on Human Rights

Switzerland is a contracting party to the European Convention on Human Rights ("ECHR"), which establishes the European Court for Human Rights ("ECtHR"). The jurisdiction of the ECtHR extends, according to article 32 of the ECHR, to all matters concerning its interpretation and application. Regarding interferences with privacy, article 8 mandates that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," with a proviso for government interference stating that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The ECtHR has identified several categories of "minimum safeguards" that ECHR contracting parties must adopt into their domestic laws to ensure effective safeguards against abuse of government powers to access electronic communications for national security purposes. These categories of minimum safeguards identified by the ECtHR are similar on the whole to the safeguards adopted in section 2(c) of Executive Order 14086. They include the grounds for authorizing surveillance; the categories of people liable to have their communications accessed; procedures for examining, using, storing, retaining, and erasing the data obtained; procedures for preserving the integrity and confidentiality of data; precautions to be taken when communicating the data to other parties; arrangements for supervising the implementation of surveillance measures and compliance with safeguards; and the remedies provided for by national law.[1] *See Roman Zakharov v. Russia*, Application no. 47143/06, §§ 233-34 (2015); *Kennedy v. the United Kingdom*, Application no. 26839/05, §§ 152-53 (2010); *Weber and Saravia v. Germany*, Application no. 54934/00, § 95 (2006); see discussion at *Centrum För Rättvisa v. the Kingdom of Sweden*, Application no. 35252/08, §§ 249-55 (2021). The ECtHR has also found it important for domestic law to require intercepting agencies to keep records of interceptions, in order to ensure that supervisory bodies have effective access to details of surveillance activities

[1] The categories of "minimum safeguards" identified by the ECHR for intelligence surveillance activities, and the requirements established by the ECtHR for each of the categories, are discussed in more detail in the memorandum published in support of designation by the Attorney General of the European Union and other countries of the European Economic Area. Department of Justice, National Security Division, *Memorandum in Support of Designation of the European Union and Iceland, Liechtenstein and Norway as Qualifying States Under Executive Order 14086*, at 5-11, available at https://www.justice.gov/opcl/executive-order-14086 ("NSD Supporting Memorandum for Designation of the EU/EEA").

undertaken. *Roman Zakharov v. Russia*, § 272; *Big Brother Watch and Others v. the United Kingdom*, Application nos. 58170/13, 62322/14 and 24960/15, § 356 (2021).

In our earlier memorandum in support of designating the EU/EAA, we assessed that the legal requirements imposed by the ECHR on the countries of the European Union and European Economic Area could be deemed to provide a basis for a section 3(f)(i)(A) determination, noting that the categories of "minimum safeguards" that the ECtHR has identified for signals intelligence activities are on the whole similar both to the principles for protecting privacy in the 2022 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities and the safeguards in Executive Order 14086 and other U.S. law.[2] That analysis is incorporated herein by reference. We noted in that analysis, however, that the jurisprudence of the ECtHR indicates what precise safeguards a country is required to enact with respect to only some of the identified categories of "minimum safeguards," while for other categories the ECtHR appears not to have specified the precise safeguards that are required, either because the ECtHR has not had occasion to do so or because the ECtHR leaves those issues to ECHR member countries' discretion.[3] Furthermore, that earlier memorandum noted that it appears that the ECtHR has thus far not applied those safeguards to signals intelligence activities occurring outside a country's jurisdiction.[4]

b. Swiss laws on signals intelligence activities and related privacy safeguards

The primary Swiss legislation authorizing signals intelligence activities and establishing related privacy safeguards is the Intelligence Services Act ("IntelSA") which governs the activities of the Federal Intelligence Service ("FIS").[5] The Swiss Paper explains that the FIS, which is administratively located within the Federal Department of Defense, Civil Protection and Sport ("DDPS"), is responsible for providing a comprehensive assessment of the national security threat situation, including through gathering information for the early detection of threats such as terrorism, violent extremism, espionage, proliferation of weapons of mass destruction and their delivery system technology, as well as cyberattacks against critical infrastructure, and information relevant to security policy abroad. The FIS also helps the Swiss cantons maintain internal security, and it supports federal law enforcement authorities, although the FIS does not itself exercise law enforcement powers. The IntelSA came into force in 2017 together with the Ordinance on the Federal Intelligence Service ("FISO"), the Ordinance on the FIS Information and Storage Systems ("ISSO-FIS"), and the Ordinance on the Supervision of Intelligence Activities ("OSIA").[6]

The IntelSA requires approvals and supervision of FIS signals intelligence activities by other government bodies and the Swiss courts. The statute requires that certain guidance and

[2] *Id.* at 32.
[3] *Id.* at 10-11.
[4] *Id.* at 13-14.
[5] An English copy of the IntelSA, including amendments through September 2023, is published by the Swiss government for information purposes only and not as an official translation. SR 121 - Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, IntelSA) (admin.ch) . The Swiss government has confirmed the accuracy of the descriptions of the IntelSA in this memorandum.
[6] These three ordinances are not available in English. The Swiss government has confirmed the accuracy of references to the ordinances in this memorandum.

approvals be provided by the Federal Council, which is the federal cabinet of the Swiss Confederation, whose seven members serve as the collective head of state and government of Switzerland. Separately, certain more intrusive FIS surveillance activities, including the surveillance of electronic communications, must be approved by the Federal Administrative Court ("FAC"), one of four federal courts in Switzerland, in addition to being cleared by the Head of the DDPS, who also serves as Minister of Defense. The judges of the FAC are elected by the United Federal Assembly of Switzerland for a term of six years, with reelections possible. As described in the Swiss Paper, although according to article 5 of the Federal Act on the Federal Administrative Court anyone entitled to vote in federal matters is eligible for election as an FAC judge, comprehensive legal training is an essential requirement in practice, and eminent lawyers are generally elected. Furthermore, according to article 30 of the Swiss Federal Constitution, the courts shall be legally constituted, competent, independent and impartial, and article 191c of the Federal Constitution states that the judicial authorities are independent in the exercise of their judicial powers and are bound only by the law. A judge may be removed from the FAC by the United Federal Assembly only if the judge has willfully or through gross negligence committed a serious violation of his or her official duties or has permanently lost the capacity to carry out his or her official duties. Finally, oversight of FIS activities is provided by the Independent Oversight Authority for Intelligence Activities ("OA-IA") and the Independent Control Authority for Radio and Cable Intelligence ("ICA"), and the United Federal Assembly exercises parliamentary oversight of the FIS through the Control Delegation.

The IntelSA sets out an overarching standard restricting the scope of the intelligence collection operations of the FIS, which is complemented by further, more detailed limitations and restrictions applicable to the specific collection measures that are authorized. The overarching standard is in article 5(3), which requires that, in each case, the FIS must choose the collection technique or measure that is most suitable and necessary for achieving a specific information gathering objective and that causes the least interference with the fundamental rights of the persons concerned.

Additionally, where the IntelSA does not establish a privacy safeguard to address a given issue, for example issues relating to the processing by the FIS of personal data acquired through intelligence surveillance, FIS activities with respect to that issue are subject to Swiss data protection law, specifically the Federal Act on Data Protection ("FADP")[7] and accompanying regulations which came into effect in September 2023. The strengthened safeguards in this new Swiss data protection framework are discussed in detail at pages 3-8 of the Swiss Paper. The independent body in charge of overseeing compliance with data protection rules by private operators and federal government agencies, including intelligence agencies, is the Swiss data protection authority, the Federal Data Protection and Information Commissioner ("FDPIC"). The FDPIC is an independent regulator. The head of the FDPIC is appointed for a four-year term by the United Federal Assembly. The United Federal Assembly may remove the head of the FDPIC from office before the end of the term only if he or she has willfully or through gross negligence committed a serious violation of his or her official duties or has permanently lost the capacity to carry out his or her official duties. FADP art. 44.

[7] Federal Act on Data Protection of 25 September 2020 https://www.fedlex.admin.ch/eli/cc/2022/491/en (unofficial English language version). The Swiss government has confirmed the accuracy of references to the FADP in this memorandum.

The following discussion begins with a description of the objectives set out in the IntelSA based on which the FIS may conduct signals intelligence activities, followed by a review of the several types of signals intelligence collection measures that are authorized in chapter 3 of the IntelSA. With respect to those collection activities, the discussion focuses on potential access by the FIS to U.S. persons' personal data that has been transferred to the territory of Switzerland; potential access to data while in transit is treated separately in a later section.[8] As in the United States under the Foreign Intelligence Surveillance Act, an independent judicial officer is required to provide *ex ante* approval, either for each individual target or at a programmatic level, for all FIS surveillance conducted within Switzerland involving the acquisition of the content of electronic communications. The discussion below of collection authorities in the IntelSA is followed by a discussion of other privacy safeguards in Swiss law relating to signals intelligence activities, including safeguards relating to the handling and sharing of data acquired through signals intelligence collection, oversight of the FIS, and individualized redress.

i. Legitimate objectives for signals intelligence activities

Similar to section 2(b)(i) of EO 14086, the IntelSA specifies legitimate objectives based on which signals intelligence activities may be authorized and conducted, in several categories. Article 6(1)(a) of the IntelSA authorizes the FIS to gather and process information to detect and prevent security threats arising from terrorism; espionage; proliferation of nuclear, biological or chemical weapons; attacks on critical infrastructure; and violent extremism. Articles 6(1)(b) and (c) then list broader objectives, authorizing the FIS to gather and process information to identify, observe and assess events outside Switzerland that are of security-policy significance and to safeguard Switzerland's capacity to act. These general objectives listed in article 6 are complemented by additional, narrower lists later in the IntelSA for the authorization of certain FIS surveillance measures. *See, e.g.*, IntelSA art. 27(1) (authorizing targeted collection through certain intrusive surveillance measures based on the specific threats listed in articles 19(a)-(d), or based on a special authorization of the Federal Council under article 3).

The Swiss government may expand the list of legitimate objectives when needed. Specifically, article 6(1)(d) of the IntelSA, read together with articles 2 and 3, provides a mechanism similar to section 2(b)(i)(B) of EO 14086 for updating legitimate objectives based on new national security imperatives. Those provisions authorize the FIS to gather and process information to safeguard other interests where the Federal Council has issued a specific mandate to do so in the event of a serious and immediate threat, in order to address a list of broadly stated Swiss interests including (i) safeguarding Switzerland's democratic and constitutional principles; (ii) protecting the freedoms of its population; (iii) increasing the security of the Swiss population and of Swiss citizens abroad; (iv) supporting Switzerland's capacity to act; (v) contributing towards safeguarding international security interests; (vi) protecting basic constitutional order in

[8] This approach was also adopted in the memorandum published in support of designation by the Attorney General of the European Union and other countries of the European Economic Area. The primary basis for this approach is that a destination country's laws and practices regarding signals intelligence activities do not uniquely govern the privacy protection that is afforded to data located outside of that country or outside of any country, as explained further in that EU/EEA memorandum and also below in section II.b.vi. NSD Supporting Memorandum for Designation of the EU/EEA at 13-14.

Switzerland; (vii) supporting Swiss foreign policy; and (viii) protecting Switzerland as a location for employment, business and finance.[9]

The IntelSA also specifies a limited set of prohibited objectives, which may not be a purpose for conducting signals intelligence activities. These prohibitions however relate only to political or speech activities in Switzerland. Article 5(5) of the IntelSA states that the FIS may not gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland. (Exceptions to this prohibition are set out in articles 5(6)-(8) for terrorist, espionage, or violent-extremist activities and organizations or groups on a watch list.) In comparison with the prohibited objectives for signals intelligence activities set out in section 2(b)(ii) of EO 14086, which apply to all U.S. signals intelligence activities and protect the privacy interests of all non-U.S. nationals, Switzerland's prohibited objectives cover narrower grounds and do not appear to protect the interests of people outside Switzerland.

ii. Intelligence collection activities authorized by the IntelSA

a) Targeted intelligence surveillance within Switzerland

Chapter 3, section 4 of the IntelSA (articles 26-33) authorizes the FIS to undertake a range of targeted signals intelligence collection activities within Switzerland with judicial approval. These activities could involve the collection by FIS of U.S. persons' personal data that has been transferred from the United States to Switzerland. The collection activities authorized by section 4 include both requesting electronic communications data from third-party providers and using direct access methods. The same court approval process and other limitations and safeguards apply to the collection activities authorized by section 4 regardless of the type of data sought, for example regardless of whether the FIS seeks to obtain content or non-content data.

Article 26 of the IntelSA lists the types of intelligence collection measures that are authorized by section 4. They include (i) surveillance of post and telecommunications, including requests for metadata in accordance with the Federal Act on the Surveillance of Post and Telecommunications ("SPTA") [10] (as explained further below); (ii) the use of special technical devices to monitor telecommunications, to record transmissions or to identify a person or object or to ascertain their location; (iii) the use of devices to establish the location and the movements of persons or objects; (iv) 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

[9] Regarding the last objective listed here—the objective of protecting Switzerland as a location for employment, business and finance—the Swiss Paper notes that a dispatch of the Federal Council on the IntelSA explains this objective by indicating that it would apply, for example, in the event of pressure directed against specific economic sectors of national importance. FF 2014 2029 - Message concernant la loi sur le renseignement (admin.ch) (not available in English). The Swiss Paper goes on to clarify that this objective would not authorize the FIS to afford a competitive advantage to Swiss companies and Swiss business sectors commercially. For example, article 23 of the FISO protects professional secrets and stipulates that the FIS must not come into possession of information related to a professional secret and unrelated to the reason for surveillance.

[10] Available at SR 780.1 - Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) (admin.ch) (unofficial English language version). The Swiss government has confirmed the accuracy of references to the SPTA in this memorandum.

accessible locations; and (v) the intrusion into computer systems and computer networks in order to gather information or disrupt, prevent or slow down access to information where the computer systems and computer networks are being used for attacks on critical infrastructures. Certain of these techniques are subject to further specified limitations and restrictions—for example, special technical devices to monitor telecommunications, record transmissions or identify a person or object or to ascertain their location may only be used if less intrusive surveillance of post and telecommunications has been unsuccessful, would be without prospect of success or would be unreasonably difficult and the licenses under telecommunications law for the special technical devices have been obtained. IntelSA art. 26(1)(abis).

Article 27(1) of the IntelSA lists three requirements to be met for the FIS to order the use of these collection techniques: (i) there must be a specific threat among those listed in IntelSA article 19(2) (terrorism; espionage; proliferation of nuclear, biological or chemical weapons; and attacks on critical infrastructure), or the measure must be required to safeguard other important national interests identified by the Federal Council in accordance with article 3; (ii) the seriousness of the threat must justify the use of the technique; and (iii) intelligence investigations to date must have been unsuccessful or would otherwise be without prospect of success or unreasonably difficult. These requirements apply in addition to the overarching provision in article 5(3), mentioned above, requiring that the FIS choose the collection technique or measure that is most suitable and necessary for achieving a specific information gathering objective and that causes the least interference with the fundamental rights of the persons concerned.

The FIS may use these intelligence collection measures only with prior judicial approval from the FAC and also the approval of the Head of the DDPS. IntelSA art. 27(2). In order to obtain judicial approval for such an intelligence collection measure, the FIS must submit to the FAC an application with details relating to (i) the specific objective of the information gathering measure and the reasons for its necessity; (ii) an explanation of why investigations have so far been unsuccessful, would be without prospect of success or would be unreasonably difficult; (iii) the persons who will be affected by the information gathering measure; (iv) a precise description of the information gathering measure and details of its statutory basis; (v) any other agencies that it intends to instruct to carry out the information gathering measure; (vi) when the information gathering measure will start and finish and the deadline by which it must be carried out; and (vii) the files and documentation supporting the application. *Id.* art. 29(1). The Swiss Paper explains that the application of these criteria requires that these intelligence collection measures be targeted at specific persons or organizations. The FAC may require a hearing with representatives of the FIS as part of its decision-making process, may grant an authorization subject to conditions, or may request further files or further investigations. *Id.* arts. 29(4)-(5). As highlighted in the Swiss Paper, when deciding on the approval of an intelligence collection measure the FAC will apply the requirement in IntelSA article 5(3) to use the information gathering measure that is most suitable and necessary for achieving a specific information gathering objective and that causes the least interference with the fundamental rights of the persons concerned, which implies that the FAC examines the proportionality of the measure as well as whether the categories of key words are necessary for the fulfillment of the order of the FIS in question. After obtaining court approval, the FIS must submit the proposed signals intelligence measure to the Head of the DDPS, which decides whether to clear the measure after written consultations with the Head of the Federal Department of Foreign Affairs ("FDFA") and

the Head of the Federal Department of Justice and Police ("FDJP"), or in cases of particular importance after referring the measure to the Federal Council. *Id.* art. 30.

Authorizations for the surveillance of electronic communications may involve the issuance by FIS of orders to third parties (such as electronic communications service providers) to disclose customer data. IntelSA art. 28. Where an FIS production order is issued to an electronic communications service provider, the provider may challenge the order in court. Article 83 of the IntelSA stipulates that rulings based on the IntelSA issued by the FIS may be contested by appeal to the FAC. Such a challenge to an FIS order does not have the effect of suspending the FIS decision. *Id.* art. 83(2). Decisions of the FAC may be appealed to the Federal Supreme Court. *Id.* art. 83(4).

Additionally, article 25(2) of the IntelSA authorizes the FIS to obtain non-content information relating to electronic communications in accordance with article 15 of the SPTA. The Swiss Paper explains that under this provision the FIS may submit a request to the Post and Telecommunications Surveillance Service ("PTSS"), a service that according to article 3 of the SPTA and under article 269 of the Code of Criminal Procedure provides surveillance upon request from law enforcement or intelligence agencies of post and telecommunications. The PTSS, which is administratively assigned to the FDJP and performs its tasks autonomously and is not subject to instructions, is empowered to obtain data from telecommunications service providers. According to the Swiss Paper, the data that may be obtained by the PTSS from telecommunications providers for the FIS is limited to basic subscriber information, such as the identity of the person registered to a phone number or electronic communications account. The Swiss Paper also explains that, in accordance with article 26(1)(a) of the IntelSA, FIS requests to the PTSS for this information must be approved by the FAC as a double authorization.

b) Foreign-focused non-individualized surveillance in Switzerland of electronic communications sent or received outside of Switzerland

A particularly relevant factor for purposes of reviewing, pursuant to section 3(f)(i)(A) of Executive Order 14086, whether the laws of Switzerland "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred" from the United States to Switzerland, is the kind of safeguards required under Swiss law for surveillance within Switzerland focused on electronic communications sent or received outside of Switzerland. As discussed in the supporting memorandum for designation of the European Union and other European Economic Area countries, a number of European countries have established special "foreign-focused" surveillance programs within their territories focused on monitoring and gathering electronic communications sent from or received abroad, which are subject to privacy safeguards that differ from the safeguards applicable to intelligence surveillance of domestic communications.[11] Similarly, the United States has also established a program for foreign-focused intelligence surveillance within U.S. territory, through Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which authorizes the U.S. government to acquire electronic communications sent or received by non-U.S. persons located outside the United States to acquire foreign intelligence information.

[11] NSD Supporting Memorandum for Designation of the EU/EEA at 16-19.

Switzerland also has such a foreign-focused intelligence surveillance program. Chapter 3, section 7 of the IntelSA (articles 39-43) authorizes the FIS to gather information about events outside Switzerland through the surveillance of electronic communications involving at least one communicant located outside Switzerland that are transmitted on cables crossing into Switzerland. If both the sender and the recipient of a communication are located in Switzerland, the communications data may not be used and must be destroyed. IntelSA art. 39(2). Operators of cable-based networks and providers of telecommunications services in Switzerland are obliged to provide the technical information and to supply communications signals, including the content of the communications, required to carry out the cable communications intelligence. *Id.* art. 43. This Swiss surveillance program could in principle be used by the FIS to acquire electronic communications sent or received by a U.S. person in the United States that are sent to or from a person in Switzerland or that are passing through Switzerland.

The IntelSA directs that the FIS shall not itself carry out the initial monitoring and filtering of the electronic communications transmitted by cable into Switzerland, but instead that the FIS may provide instructions for those purposes, after review and approval by the FAC, to a separate service, which the Swiss Paper identifies as the Service for Actions in Cyberspace and Electromagnetic Space ("ACEM"). Based on those instructions, the ACEM filters the electronic communications transmitted by cable into Switzerland and removes some data by applying several criteria before providing data to the FIS. First, the ACEM may only pass data to the FIS that match a list of search parameters that are provided by the FIS in the form of key words necessary for the fulfillment of the instructions provided by the FIS after approval by the FAC. IntelSA arts. 39(3), 42(2). Key words in the form of information about Swiss persons may not be used as search parameters. Although it appears that key words in the form of information about U.S. persons or other non-Swiss persons may be used as search parameters, the search parameters must in all cases be chosen to minimize interference with the private domain of all persons. *Id.* art. 39(3). Second, as mentioned above, if both the sender and the recipient of a communication are located in Switzerland, the communications data may not be used and must be destroyed. *Id.* art. 39(2). Third, information about persons in Switzerland may be passed by the ACEM to the FIS only if the data is anonymized and necessary to understand an event abroad. *Id.* art. 42(2). If however the data pertains to a specific threat listed under article 6(1)(a) (terrorism, espionage, arms proliferation, attacks on critical infrastructure, and violent extremism), the ACEM may pass the data to the FIS unchanged. *Id.* art. 42(3). The Federal Council, pursuant to IntelSA art. 39(4), has issued secondary legislation to regulate this surveillance program in terms of the permitted fields of communications intelligence; the organization and the details of the procedure for cable communications intelligence; and the maximum period that the ACEM may retain recorded content and connection data obtained from cable communications intelligence. FISO art. 25 ff.

This foreign-focused intelligence surveillance program requires prior approval at a programmatic level from both the FAC and the Head of the DDPS. IntelSA art. 40(2). In order to obtain judicial approval, the FIS must submit to the FAC an application with (i) a description of the mandate to be issued to the ACEM; (ii) the reasons why the operation is necessary; (iii) details of the categories of the search parameters in the form of key words that the ACEM will use to conduct the surveillance by identifying electronic communications the content of which matches the key words; (iv) 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 (v) details of when the operation will start and finish. *Id.* art. 41(1). The FAC does not review each individual key word that the FIS will provide to the ACEM for the filtering of electronic communications passing by cable into Switzerland; rather, as explained in the Swiss Paper and in accordance with IntelSA article 41(1)(c), the FAC reviews and approves information in the FIS submission that describes the categories of the key words to be used. The court may require a hearing with representatives of the FIS as part of its decision-making process, may grant an authorization subject to conditions, or may request further files or further investigations. *Id.* arts. 29(4)-(5), 41(2).

By gathering electronic communications not by targeting specific persons' communications accounts based on individualized suspicion that their communications will contain information of intelligence interest, but instead through the use of search parameters in the form of key words on topics of intelligence interest, this Swiss surveillance program operates as a form of bulk collection as that term is understood in U.S. law.[12] Executive Order 14086 defines "bulk collection" as "the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)." EO 14086 § 4(b). In this respect, this Swiss program differs from U.S. law, which prohibits bulk intelligence surveillance domestically, and the Swiss program specifically differs from the U.S. program for foreign-focused intelligence surveillance under FISA Section 702, which authorizes the acquisition of electronic communications only of specifically targeted persons.[13] However, the program is subject to multiple privacy safeguards in the IntelSA including the requirement in article 39(3) that the key words used to obtain electronic communications data be defined so that their application causes as little interference as possible in the private domain of persons. Additionally, the Swiss Paper states that in the implementation of this program it is "more effective and less intrusive to search for specific personal details of a targeted person or for a telecommunications connection used by a targeted person than using a trivial search term."

It appears that the IntelSA itself places few restrictions on how the FIS may query or search the large volumes of data that match the search parameters that are passed to it by ACEM after triaging and filtering of the data forwarded from the cable networks. IntelSA arts. 42(1)-(2). As explained in the Swiss Paper, however, other Swiss law restricts how FIS may query the data. First, as a public authority the FIS is bound by the constitutional requirement that all administrative action must be lawful, proportionate and in accordance with the principle of good faith. Swiss Federal Constitution art. 5. Second, and more specifically, when processing personal data the FIS must comply with the principles and obligations set by applicable data protection legislation, the FADP, which effectively establishes restrictions on querying of

[12] The European Court of Human Rights appears to have similarly characterized this Swiss program as involving bulk surveillance. *Centrum För Rättvisa v. the Kingdom of Sweden*, § 131 ("At least seven Contracting States (being Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways.").

[13] While Section 702 safeguards differ from the individualized court approvals required under other sections of FISA for electronic surveillance of persons located in the United States, the Section 702 program operates only on a targeted basis, authorizing the acquisition of the electronic communications of specific persons based on written justifications, with each individual targeting decision and rationale reviewed through independent oversight. *See* NSD Supporting Memorandum for Designation of the EU/EEA at 16-19.

personal data for intelligence purposes. Specifically, according to the principles of legality and good faith, the FIS may only process personal data if and to the extent authorized by law. FADP arts. 6(1)-(2). In addition, the principle of proportionality obliges the FIS to process personal data only to the extent that is suitable to achieve the required purpose and to process only data that is necessary for this purpose. *Id.* art. 6(2). The purpose of the data processing must be proportionate to the interference with fundamental rights, which requires a balancing of the private interest of the person concerned and the public interest in processing personal data. Further, the purpose limitation obliges the FIS to process personal data only within its competence and for a legally prescribed purpose. *Id.* art. 6(3). Finally, the FIS must apply all necessary technical and organizational measures in order to ensure data security and integrity. *Id.* art. 8. (These same constitutional and FADP restrictions apply to the ACEM's initial processing of the data.) The Swiss Paper emphasizes that the FAC will assess compliance with these data protection principles when deciding on the approval of surveillance measures.

iii. Post-Acquisition Handling of Data

The IntelSA contains numerous provisions restricting the handling of data acquired by the FIS through signals intelligence collection. For example, with respect to data quality and security, the FIS is required to assess the relevance and accuracy of personal data before recording it in its information systems and only to record data that may be used to fulfil its tasks as defined by the IntelSA. IntelSA art. 45(1)-(2). The FIS is also required to store data acquired through the targeted surveillance authorized under chapter 3, section 4 on a case-related basis and separately from the general information systems operated by FIS. *Id.* art. 58(1).

Regarding the retention and deletion of data acquired, the FIS is required to periodically check in all of its information systems whether the recorded sets of personal data are still required to carry out the tasks of the FIS and to delete data records that are no longer required. IntelSA art. 45(4). The FIS also must ensure that personal data that was acquired through the targeted surveillance authorized under chapter 3, section 4 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. *Id.* art. 58(2). Further retention periods for specific programs and information systems are set out in the ISSO-FIS. For example, the Swiss Paper explains that the FIS must erase personal data that were gathered under the targeted surveillance authorized by Chapter 3, Section 4, and which are not used in judicial proceedings or in an ongoing operation: (a) no later than 6 months after the notification of the measure to the data subject concerned under IntelSA art. 33(1); (b) immediately after the entry into force of the decision on an exemption from the obligation to notify the data subject under IntelSA art. 33(3); or (c) immediately after the entry into force of a decision on an appeal against the ordering of a measure. ISSO-FIS art. 70(1). For data gathered from surveillance authorized by chapter 3, section 6 of the IntelSA (discussed below), the maximum retention period is three years. ISSO-FIS art. 70(3). For data gathered through the foreign-focused non-individualized cable-based collection authorized by chapter 3, section 7 of the IntelSA, the Swiss Paper explains that the maximum retention period depends on the system where data is stored, with the longest retention period being forty-five years.

The IntelSA contains detailed provisions on the dissemination of data acquired through intelligence surveillance. Before disclosing any personal data, the FIS must ensure that the

access to and processing of the personal data met the legal requirements of the statute and that the disclosure is lawful and necessary in the case concerned. IntelSA art. 59. Regarding information sharing for law enforcement or other internal security purposes, the FIS may disclose personal data if the disclosure is necessary in order to safeguard internal or external security, and only to domestic authorities that are pre-approved by the Federal Council. IntelSA art. 60(1); FISO art. 32(1), annex 3 (listing authorities to whom the FIS may disclose personal data). The FIS is also authorized to disclose information that may be used by other domestic authorities for purposes of prosecuting offenses, preventing serious offenses or maintaining public order, either upon request or without request, and the FIS must always disclose data acquired through targeted surveillance under Chapter 3, Section 4 to a prosecution authority if it contains specific evidence of an offense where the prosecution authority would have been entitled to order a comparable criminal procedural investigative measure. IntelSA arts. 60(2)-(3).

The Swiss Paper describes how the FIS pursuant to the IntelSA and article 3 of FISO is further authorized to share information with the Swiss Armed Forces Intelligence Service. The two organizations are mandated to cooperate closely in areas of overlapping missions, and to support each other in the performance of the missions assigned to them, in particular by the regular transmission of information and assessments in areas of overlapping missions, and each service may request information from the other at any time. Furthermore, the Swiss Paper states that the FIS pursuant to article 4 of the FISO supports the Swiss Military Security Service including by sharing information to protect the armed forces against espionage, sabotage and other illegal acts.

The IntelSA sets out additional standards for dissemination by the FIS of personal data to foreign governments. The FIS may disclose personal data electronically to foreign security agencies from countries that guarantee an adequate level of data protection according to article 16(1) of the FADP or an appropriate standard of data protection where Switzerland has concluded a relevant agreement with the country. IntelSA art. 61(1)-(2). For countries that do not guarantee an adequate level of data protection and no such agreement has been concluded, the FIS may disclose information only if Switzerland maintains diplomatic relations with the country and either (i) Switzerland is required by law or by an international agreement to disclose the personal data; (ii) disclosure is required to safeguard an overriding public security interest in Switzerland or in the receiving state; (iii) disclosure is necessary in order to justify a request for information from Switzerland; (iv) disclosure 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; or (v) disclosure is necessary in order to protect the life and limb of third parties. *Id.* art. 61(2). Furthermore, the FIS may not disclose personal data to a foreign security agency if the person concerned will be exposed to the risk of being sentenced twice for the same offense or of serious harm to his or her life, limb or freedom in violation of international agreements that Switzerland has ratified. *Id.* art. 61(5).

The FIS may disclose personal data to non-government third parties only if either (i) the person concerned has consented to disclosure or disclosure is indisputably in the interest of the person concerned; (ii) disclosure is necessary in order to repel a serious immediate danger; or (iii) disclosure is necessary in order to justify a request for information. IntelSA art. 62.

iv. Oversight

The intelligence activities of the FIS and the ACEM are supervised by the Independent Oversight Authority for Intelligence Activities ("OA-IA"), which was established in 2017 pursuant to article 76 of the IntelSA. The OA-IA monitors and audits the legality, the expediency and the effectiveness of FIS and ACEM activities. IntelSA art. 78(1).

Additionally, a separate oversight body, the Independent Control Authority for Radio and Cable Intelligence ("ICA"), which was established in 2003, provides additional oversight of radio and cable surveillance, including the foreign-focused non-individualized surveillance within Switzerland of electronic communications sent or received abroad that is authorized under chapter 3, section 7 of the IntelSA as discussed above. IntelSA art. 79. The ICA is responsible for verifying the legality of radio communications intelligence and supervising the conduct of authorized and cleared cable communications intelligence instructions. *Id.* art. 79(1). In particular, the ICA examines the instructions and the key words given to the ACEM and the processing and passing to the FIS of information by the ACEM. Its organization and tasks are governed by the Ordinance on the Supervision of Intelligence Activities ("OSIA").[14]

The OA-IA operates independently. It is given statutory independence, is not bound by directives from other authorities, has its own budget and staff, and regulates its own organization and working methods in its own procedural rules. IntelSA art. 77. The Federal Council appoints the head of the OA-IA for a renewable period of six years and may remove him or her only for willful breach of official duties, gross negligence, or permanent incapacity. *Id.* art. 76. The ICA also has significant attributes of independence. It is not bound by directives from other authorities in carrying out its tasks. *Id.* art. 79(1). The Swiss Paper explains that the Federal Council appoints its members for terms of office of four years, and that the Federal Council may remove ICA members only for cause, based on the same grounds listed above for removal of the head of the OA-IA. As an internal administrative commission, it consists of three to five officials from the federal administration with expertise in the areas of fundamental rights protection, security policy and communications technology. OSIA arts. 7(1)-(2). The Federal Council is responsible for regulating its composition and the organization, the remuneration of its members, and the organization of its Secretariat. *Id.* arts. 7(3)-(4). Decisions of the ICA require the approval of the majority of its members. *Id.* arts. 8(1)-(3).

The OA-IA and ICA are granted access by statute to the information needed to carry out their mandates. The OA-IA may have access to all the information systems and databases of the subjects of supervision; it may also have access to sensitive personal data. IntelSA art. 78(5). Additionally, within the scope of its supervision activities, the OA-IA may request documents and 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. *Id.* art. 78(4). The ICA, with respect to its statutory responsibility to examine the instructions given to the ACEM and the processing and passing on to the FIS of information,

[14] RS 121.3 - Ordonnance du 16 août 2017 sur la surveillance des activités de renseignement (OSRens) (admin.ch) (not available in English). The Swiss government has confirmed the accuracy of references to the OSIA in this memorandum.

must also be granted access by the responsible agencies to all relevant information and facilities. *Id.* art. 79(2). The FIS is obliged to notify the ICA of every new radio and cable intelligence order and to provide the ICA with all necessary information. OSIA art. 9(1). The Swiss Paper explains that in the exercise of its control mandate, the ICA may view relevant orders, applications and decisions with respect to cable intelligence, examine results of radio and cable intelligence on a random basis or examine the ACEM procedures, data and systems. *Id.* art. 10(1). In principle, radio and cable intelligence orders must be audited on an annual basis. *Id.* art. 10(2). The Swiss Paper notes that as part of its audit activities, the ICA carries out inspection visits to the competent bodies several times a year.

As confirmed in the Swiss Paper, both the OA-IA and the ICA are authorized to initiate audits either in response to corresponding requests or acting on their own volition. OSIA art. 10(1)(c)-(f). The OA-IA publishes an annual activity report describing its oversight of FIS activities including information collection, data processing, coordination with the cantons, and implementation of OA-IA recommendations.[15] The OA-IA annual report for 2022 refers to 19 audits that the OA-IA worked on that year on a range of topics as well as the OA-IA's outreach to other relevant Swiss government offices and to the FAC to discuss "the court's rejection and authorization of information gathering measures."[16] Among numerous examples, the report discusses a compliance incident involving collection of information by the FIS for which FAC approval was required but not obtained, for which the FIS director appropriately directed the termination of the collection and other remedial steps such as increased training and administrative restructuring.[17] Regarding the ICA, the Swiss Paper explains that the ICA submits an annual report on its activities and the audit results to the Head of the DDPS, who sends the report to the Federal Council and informs it about the recommendations of the ICA and their implementation. OSIA art. 10(3). The results of the ICA's audit activities are confidential and are submitted only to the bodies provided by law, or bodies affected by the subject matter, which are the Federal Council, the Control Delegation of the Federal Assembly, the OA-IA and the FAC. Neither the reports of the ICA nor its recommendations or proposals are public. IntelSA art. 79(3).

The OA-IA is required to provide the DDPS with a written report on the results of its audits, which may include remedial recommendations. IntelSA art. 78(6). The Head of the DDPS is then required either to accept each recommendation and ensure that it is implemented by the FIS, or, if the DDPS rejects a recommendation, to report the rejection to the Federal Council for a decision. *Id.* art. 78(7). If they are accepted, they are binding and must be implemented by the FIS. The Swiss Paper indicates that to date, all of the OA-IA's recommendations have been accepted. The OA-IA annual report for 2022 notes that the intelligence services have implemented 150 of those accepted recommendations since the OA-IA was established in 2017, with 19 recommendations to the FIS pending.[18] The Swiss Paper also notes that the OA-IA is informed about the implementation of the recommendations by the DDPS, and if it is not satisfied with the information received, the OA-IA can carry out a new audit, which may lead to a further recommendation. The ICA may also issue non-binding

[15] The annual reports of the OA-IA are available at this link (admin.ch) .
[16] Annual Report 2022 of the Independent Oversight Authority for Intelligence Activities OA-IA at 6, 24.
[17] *Id.* at 19.
[18] *Id.* at 20.

recommendations based on its audits and request that the DDPS terminate radio communications or cable intelligence instructions and delete information. Its recommendations, requests and reports are not made public. IntelSA art. 79(3).

Oversight of Swiss intelligence activities is supported by documentation requirements. For example, with respect to information gathering about events outside Switzerland authorized by chapter 3, section 6 of the IntelSA (discussed below), the FIS must document information gathering about events outside Switzerland for the attention of the supervision and control bodies. IntelSA art. 36(4). The Swiss Paper explains that the IntelSA does not set out such provisions for the recording of processing activities with respect to some other types of authorized intelligence activities, such as those activities authorized by sections 4 and 7 of chapter 3 of the IntelSA. Those activities are accordingly subject to the general documentation requirements in Swiss data protection law, specifically article 12 of the FADP which requires recording, among other categories of information, the purpose of data processing, a description of the categories of data subjects and the categories of processed personal data, and the categories of recipients of the data. The FIS is also required to notify the FDPIC of its records of its data processing activities. Furthermore, the Swiss Paper explains that the FIS is obliged to provide evidence of its activities that are supported by business management systems. Ordinance of 25 November 1998 on the Organization of the Government and the Federal Administration ("GAOO")[19] art. 22 (implementing IntelSA art. 52). The Swiss Paper notes that OA-IA bases its oversight on this latter documentation requirement.

The above oversight of FIS by the OA-IA and the ICA does not exclude the supervisory powers of the independent FDPIC, which is entitled to and has a legal obligation to monitor legal conformity of personal data processing with Swiss data protection law by federal government agencies including the FIS. The FDPIC may initiate an investigation on its own initiative or upon request of a third party with respect to both private operators and any federal government agency. FADP art. 49(1). In carrying out its investigations, the FDPIC has access to all relevant information. *Id.* arts. 49(3), 50(1). The FDPIC has the power to adopt binding decisions with respect to both private operators and federal agencies, including to order them to modify, suspend or terminate processing or destroy personal data. *Id.* art. 51. The FDPIC has to date not carried out any formal investigations of the FIS. However, as noted, the FDPIC has the authority to open an investigation on its own volition based on the FADP and can supervise the FIS without restriction, just like any other federal agency.

v. Individualized redress

A U.S. person who is concerned that the FIS has unlawfully gathered and processed his or her personal information that has been transferred from the United States to Switzerland has several avenues for submitting a complaint under Swiss law.

[19] RS 172.010.1 - Ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA) .

If the person is aware of FIS surveillance or other activities that have affected him or her, he or she may bring a legal challenge to them as a "ruling"[20] of the FIS before the FAC, with appeal to the Federal Supreme Court. IntelSA arts. 83(1)-(4). A person could file such a lawsuit based on evidence of FIS surveillance activities, for example, after the person is notified by the FIS of surveillance activity affecting him or her pursuant to notification requirements in the IntelSA. Those IntelSA notification requirements are, however, subject to several exceptions. Most importantly for purposes of this assessment, notification is required only for the targeted surveillance authorized by chapter 3, section 4 of the IntelSA, and not for the foreign-focused non-individualized surveillance authorized by chapter 3, section 7. The FIS is required to notify a person who is subject to the targeted surveillance authorized by chapter 3, section 4 within one month after the conclusion of an operation of the reason for and nature and duration of the surveillance. *Id.* art. 33(1). The FIS may postpone or dispense with giving such notification, with authorization by the FAC and head of DDPS, when (i) necessary to avoid jeopardizing ongoing surveillance or a legal proceeding; (ii) necessary due to another overriding public interest in order to safeguard internal or external security or Swiss foreign relations; (iii) notification could cause serious danger to third parties; or (iv) the person concerned cannot be contacted. *Id.* arts. 33(2)-(3).

Separately, a person may file a legal challenge not against specific signals intelligence activities affecting him or her, but instead challenging an aspect of Switzerland's signals intelligence legal regime as a whole, without having to prove that the FIS accessed his or her information. This right was recently confirmed by the Federal Supreme Court with respect to the foreign-focused non-individualized surveillance program authorized by Chapter 3, section 7.[21] According to the Swiss Paper, the private Swiss association *Digitale Gesellschaft*, a non-profit association established for the protection of citizens and consumers, claimed that the operation of radio and cable surveillance by the FIS and other agencies, in particular the ACEM, violates its fundamental rights such as the right to and protection of privacy, protection against the misuse of personal data and to informal self-determination, freedom of assembly and the presumption of innocence. The Supreme Court referred the case back to the FAC, instructing the FAC to examine whether the presumed processing of data in the current radio and cable intelligence program violates the fundamental rights of the plaintiffs under the Federal Constitution and the ECHR, and if so, to decide the legal consequences. The case is pending with the FAC.

Switzerland also provides a non-judicial redress mechanism for persons seeking to challenge the lawfulness of FIS signals intelligence activities affecting their personal data. This non-judicial redress mechanism provides a path to redress for persons who are unable to show that their own data was gathered or processed by the FIS and thus are likely to have a complaint in Swiss courts dismissed for lack of the necessary legal interest. This scenario is analogous to the type of complaint addressed by the redress mechanism established by EO 14086. In

[20] Article 83(1) of the IntelSA authorizes court challenges only to "rulings" of the FIS. The Swiss Paper advises that for this purpose the term "ruling" is defined in article 5 of the Federal Act on Administrative Procedure (APA) as a decision by a government authority relating to, inter alia, the determination of rights or obligations. If an individual sought to challenge an FIS surveillance activity that did not constitute a ruling, but instead constituted an "administrative act," the individual could request that the FIS discontinue, revoke, or rectify any unlawful acts or confirm the illegality of such acts. The FIS would then be obligated, under article 25*a*(2) of the APA, to respond to the request by way of a ruling, which could then be challenged under article 83(1) of the IntelSA.

[21] Decision 1C_377/2019 of 1 December 2020.

Switzerland, this type of complaint must initially be filed under Swiss data protection laws. Any person, regardless of nationality and with no requirement to show that the federal agency has accessed or is holding his or her data, may request that a federal agency (including the FIS), among other things, ascertain that the agency's processing of the person's data is lawful. FADP art. 25. As part of such a complaint, the person may also assert a right of access to data concerning him or her, for example data processed on the FIS's information systems. This right of access is governed by the FADP for certain FIS information systems and by the IntelSA for the remaining information systems. IntelSA arts. 63(1)-(2). The FIS may defer its response to a request for an individual's access to data based on (i) overriding interests in preserving secrecy in relation to the data in connection with a task being fulfilled in accordance with article 6 of the IntelSA, a prosecution, or other investigation; (ii) overriding interests of third parties; or (iii) if no data about the applicant has been processed. *Id.* art. 63(2).

If the FIS defers the request for access to data, the complainant, regardless of nationality, has the right to request that the FDPIC examine whether the data, if any, was or is being lawfully processed by the FIS and whether overriding interests in preserving secrecy justified the FIS's deferral. IntelSA art. 63(3). The FDPIC, which is an independent entity as explained above, will then conduct an investigation. *Id.* art. 64(1). The Swiss Paper explains that the examination by the FDPIC may cover any form of signals intelligence authorized by the IntelSA.

The FDPIC has full access to classified information necessary to its examination of a complaint, including classified information. After the FDPIC opens an investigation into a federal agency, the federal agency, which may include an intelligence agency, is obligated to provide the FDPIC with all the information and documents necessary for the investigation. FADP art. 49. Should the federal agency fail to fulfil this obligation, the FDPIC may order various measures, including production of all information, documents, records of processing activities and personal data that are required for the investigation; access to premises and installations; questioning of witnesses; and appraisals by experts. *Id.* art. 50.

Unlike the redress mechanism established under EO 14086, the Swiss redress mechanism does not require the appointment of a special advocate in each case who is authorized to access the full case record, including sensitive national security information, and is responsible for advocating for the interests of the complainant before the entity reviewing the complaint.

Upon completing its review, the FDPIC is authorized to issue a binding ruling to the FIS through a variety of remedial measures. FADP art. 51. Additionally, the IntelSA specifies that if the FDPIC identifies errors made when processing the data or when deferring the provision of information, it shall order the FIS to rectify the same. IntelSA art. 64(4).

At the end of the review process, similar to the redress mechanism established by Executive Order 14086, due to secrecy requirements for Swiss signals intelligence activities, the complainant is provided only limited information. The FDPIC is required to provide the complainant a standard notification stating that either no personal data relating to the complainant has been unlawfully processed, or the FDPIC has identified errors relating to the deferral of the provision of information and has opened an investigation under article 49 FADP.

Id. art. 64(2). This notification must be in a standard format that does not contain a statement of reasons and may not be contested or appealed, including in court. *Id.* art. 66.

vi. Safeguards applicable to FIS access to data in transit

The United States and other countries have consistently taken the position that access to data in transit between countries by the intelligence agencies of the destination country should not be a relevant consideration for the regulation of commercial flows of data.[22] The primary basis for this position is that a destination country's laws and practices regarding signals intelligence activities do not uniquely govern the privacy protection that is afforded to data located outside of that country or outside of any country. Rather, assessing possible privacy interferences with data while in transit would require reviewing the widely divergent laws and practices of many other countries than the destination country, and also the possibility of illicit access by a wide range of private actors. Accordingly, in determining whether the laws of Switzerland "require appropriate safeguards" for data "that is transferred from the United States to the territory of" Switzerland for purposes of section 3(f)(i)(A), it is reasonable to exclude from consideration whether Swiss laws require appropriate safeguards for signals intelligence activities not conducted in the territory of Switzerland. For these reasons, the above analysis of Swiss laws has focused on the domestic signals intelligence activities of the FIS, conducted within the territory of Switzerland. Nevertheless, for purposes of completeness and demonstrating Switzerland's overall commitment to privacy in this area, we review briefly here the privacy safeguards in Swiss law for extraterritorial signals intelligence activities.

Chapter 3, section 6 (articles 36-38) of the IntelSA authorizes the FIS to conduct signals intelligence activities, including activities conducted outside of Switzerland, to access data about events outside Switzerland. Several specified types of intelligence activities are authorized. For example, article 37 authorizes two types of intrusions, including through FIS activities conducted outside of Switzerland, into computer systems located abroad: article 37(1) authorizes intrusions, based on decisions of the Federal Council, into computer systems located abroad that are being used to carry out attacks on critical infrastructure in Switzerland; and article 37(2) authorizes intrusions, with the approval of the Head of the DDPS after consultation with the Head of the FDFA and the Head of the FDJP, into computer systems and computer networks outside of Switzerland in order to gather information about events outside Switzerland.[23] Additionally, article 38 authorizes the operation by a third party of a service for recording

[22] *See, e.g.*, U.S. Government White Paper, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after* Schrems II at 17-18 (2020), *available at* https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF ; United Kingdom, Department of Science, Innovation and Technology, *Analysis of the UK Extension to the EU-US Data Privacy Framework* at 55 (2023), *available at* Analysis of the UK Extension to the EU-US Data Privacy Framework (publishing.service.gov.uk) .

[23] The availability of section 6 to authorize intelligence activities conducted both domestically and outside of Switzerland is made clear by provisions in article 36, the opening article of section 6. For example, sections (6)-(7) of article 36 discuss the protection of FIS employees deployed abroad. Additionally, in discussing what rules govern the exercise of the activities authorized, article 36(2) distinguishes between activities conducted domestically and abroad, by clarifying that where FIS is gathering information inside Switzerland about events outside Switzerland, it must follow the requirements for targeted, FAC-approved surveillance set forth in chapter 3, section 4, with the exception of the intrusion authorized by article 37(2) into computer systems and computer networks outside of Switzerland in order to gather information about events outside of Switzerland.

electro-magnetic emissions from telecommunications systems located abroad (radio communications intelligence), based on Federal Council regulations, to gather information 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; as well as safeguarding of other important national interests based on a special authorization of the Federal Council under article 3. IntelSA art. 38(2). As with the foreign-focused domestic surveillance authorized under chapter 3, section 7 of the IntelSA discussed above, this radio communications intelligence must be foreign-focused: the third-party operator may pass to FIS only information relating to events outside Switzerland that are of significance to security; and may only pass on information about persons in Switzerland if the information is required to understand an event abroad and has been anonymized beforehand. *Id.* art. 38(4).

Similar to U.S. extraterritorial intelligence collection authorized by EO 12333, these Swiss extraterritorial intelligence collection activities authorized by chapter 3, section 6 of the IntelSA do not require FAC or other court approval. The governing legal standard that is specific to section 6 is that the FIS must ensure that the risk[24] 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. IntelSA art. 36(3). This is in addition to the overarching article 5(3) requirement, mentioned above, to choose the collection technique or measure that is most suitable and necessary for achieving a specific information gathering objective and that causes the least interference with the fundamental rights of the persons concerned. These overarching requirements in article 5(3) reflect a similar policy intent to the principles of necessity and proportionality for U.S. signals intelligence activities as set out in sections 2(a)(ii)(A) and (B) of EO 14086. Beyond these standards, there do not appear to be guidelines in Swiss law comparable to those in EO 14086 specifically addressing, for example, whether extraterritorial collection must prioritize targeted collection over bulk collection, or establishing specific standards under which extraterritorial collection of data in bulk may be conducted. The Swiss government advises that these extraterritorial intelligence activities authorized by section 6 are subject to the same data protection restrictions, post-acquisition data handling rules, and FIS oversight regime, and may be challenged through the same redress process, as discussed above for the domestic intelligence activities of the FIS.

c. Assessment

The Attorney General must determine for purposes of section 3(f)(i)(A) of Executive Order 14086, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, whether the laws of Switzerland "require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory" of Switzerland. As discussed above, section 3(f)(i)(A) does not require that the laws of Switzerland afford identical or reciprocal safeguards to those afforded by the United States. Rather, the required safeguards must be "appropriate."

[24] The Swiss government advises that the relevant "risk" in this context is operational or political risk—for example, risk of an operation being discovered, or risk of damage to the international standing or reputation of Switzerland.

The above discussion shows that intelligence laws in the United States and Switzerland are similar in many respects, although they differ in other respects. The laws of both countries list the legitimate purposes based on which signals intelligence activities may be conducted, with the option of the executive arm of the government expanding that list to address national security imperatives. In both countries, domestic access by intelligence agencies to the content of individuals' electronic communications requires prior review and approval, at either an individual or programmatic level, by an independent judicial officer. Additionally, the laws of both countries impose restrictions on the handling of data collected for intelligence purposes, require oversight of intelligence agencies, and provide individuals a path to independent and binding redress. Regarding individualized redress, both countries provide an independent, non-judicial redress mechanism that does not make investigation of a complaint dependent on the complainant demonstrating that his or her data was subject to surveillance. In both countries, the redress mechanism preserves the confidentiality of national security information by authorizing, upon completion of the investigation of the complaint, a standard notification that does not reveal whether the individual was subject to signals intelligence activities.

There are certain areas where the laws of the United States and Switzerland diverge, and in some areas Swiss law either authorizes more expansive surveillance than U.S. law or has less restrictive safeguards. In particular, Swiss law includes a foreign-focused intelligence surveillance program that involves the acquisition of electronic communications passing into Swiss territory based on key words of topical interest. This authorization to acquire electronic communications based on topical search terms, and not limited to collection based on individualized suspicion that a specifically targeted person will be communicating information of foreign intelligence interest, constitutes bulk collection as that term is used in U.S. law, and contrasts with the prohibition in U.S. law on bulk collection domestically for intelligence purposes. However, this Swiss program is subject to multiple privacy safeguards, including a statutory requirement that key words be defined so that their application causes as little interference as possible in the private domain of persons. Moreover, the general Swiss legal regime for signals intelligence activities includes comprehensive and detailed privacy safeguards, which demonstrate Switzerland's clear commitment to the protection of privacy with respect to its national security activities. Safeguards of particular relevance to the foreign-focused non-individualized intelligence surveillance program include querying limitations and documentation requirements—although, in contrast to the United States, these limitations and requirements are not specifically formulated for use in connection with that surveillance program but rather derive from general provisions under Swiss data protection laws. Additionally, the foreign-focused non-individualized intelligence surveillance program, like all Swiss intelligence surveillance programs, is subject to proactive oversight by independent oversight bodies conducting numerous audits annually and providing transparency of their audits through regularly published reports. Additionally, with respect to any Swiss intelligence program, individuals may seek and obtain redress from the FDPIC for complaints concerning the acquisition or handling by the FIS of their personal data, and as noted above the foreign-focused non-individualized surveillance program can also be challenged before Swiss courts.

Based on the above analysis, it is reasonable and within the Attorney General's discretion to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that notwithstanding certain areas of divergence between the

laws of the United States and the laws of Switzerland, the laws of Switzerland require appropriate safeguards for purposes of a section 3(f)(i)(A) determination.

III. Determination that Switzerland permits, or is anticipated to permit, commercial data transfers to the United States

The second determination to be made to designate Switzerland, pursuant to section 3(f)(i)(B) of Executive Order 14086, is that Switzerland permits, or is anticipated to permit, the transfer of personal information for commercial purposes between the territory of Switzerland and the territory of the United States.

On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its judgment in the "*Schrems II*" case. Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (2020). That judgment invalidated the adequacy decision issued by the European Commission in 2016 which concluded that the United States provides safeguards for government access to data, including signals intelligence activities, that are "essentially equivalent" to safeguards afforded in the EU. On September 8, 2020 the FDPIC (which had developed an indicative list of countries that provide an adequate level of data protection under the FADP of 1992, which is no longer in force) issued a policy paper in light of the *Schrems II* judgment reassessing the protection provided by the Swiss-U.S. Privacy Shield Framework and concluding it does not provide an adequate level of protection for data transfers from Switzerland to the United States pursuant to the FADP. Since the entry into force on September 1, 2023 of the FADP of 2020 and the related Data Protection Ordinance ("DPO"), it is now the responsibility of the Federal Council to determine the adequacy of the data protection offered by another country. The countries that guarantee an adequate level of data protection are listed in Annex 1 to the DPO; the United States is currently not included in this list. With respect to the possibility of Swiss data exporters relying on other transfer instruments under Swiss law (in particular standard contract clauses), the absence of the United States on the list of Annex 1 to the DPO may influence, as the FDPIC policy paper may have previously influenced, how Swiss data exporters evaluate whether U.S. law provides sufficient privacy protections in the conduct of signals intelligence activities to permit transfers of personal data to the United States. These circumstances are sufficient to place in doubt whether Switzerland currently meets the requirement of section 3(f)(i)(B) of Executive Order 14086.

The strengthened safeguards for signals intelligence activities in Executive Order 14086 were designed to address the concerns of the CJEU as set out in the *Schrems II* decision. Based on those strengthened safeguards, the European Commission on July 10, 2023 adopted an adequacy decision for the United States under the EU-U.S. Data Privacy Framework. Switzerland is likewise working towards recognizing the adequacy of protection provided by the Swiss-U.S. DPF, which will permit under Swiss law the transfer of personal information for commercial purposes in reliance on the Swiss-U.S. DPF between the territory of Switzerland and the territory of the United States. An essential step for Switzerland's recognition of adequacy is that the Attorney General designate Switzerland as a qualifying state to make the redress mechanism established by Executive Order 14086 available to Swiss individuals.

Section 3(f)(i) of Executive Order authorizes designation either "effective immediately or on a date specified by the Attorney General . . . ." Further, section 3(f)(i)(B) authorizes designation if the country "permit[s], *or [is] anticipated to permit*, the transfer of personal information for commercial purposes . . . ." (emphasis added). As noted above, based on the enhanced safeguards in Executive Order 14086, Switzerland is anticipated to recognize the adequacy of protection provided by the Swiss-U.S. DPF for the transfer of personal information for commercial purposes in reliance on the Swiss-U.S. DPF. There is accordingly a sufficient basis to determine, in light of the standard in section 3(f)(i)(B), and in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that Switzerland is anticipated to permit the transfer of personal information for commercial purposes in reliance on the Swiss-U.S. DPF between the territory of Switzerland and the territory of the United States, and, further, to make the designation of Switzerland on a contingent basis, so that the designation will come into effect upon the entry into force of Switzerland's recognition of adequacy for the United States—that is to say, upon the listing, in Annex 1 to the DPO, of the United States for data transferred for commercial purposes in reliance on the Swiss-U.S. DPF.

IV. Determination that designation of Switzerland would advance U.S. national interests

The third determination to be made to designate Switzerland, pursuant to section 3(f)(i)(C) of Executive Order 14086, is that the designation would advance the national interests of the United States. Designating Switzerland is an essential step in bringing into place the Swiss-U.S. DPF, which will provide vital benefits to citizens and businesses in both the United States and Switzerland. The Swiss-U.S. DPF will enable the continued flow of data that underpins the $660 billion U.S.-Swiss economic relationship and will enable businesses of all sizes to compete in each other's markets. There are accordingly sufficient grounds to conclude, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of National Intelligence, that it is in the national interest to designate Switzerland as a qualifying state.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

12 March 2024

Overview of Swiss data protection and safeguards for signals intelligence activities

Overview of Swiss data protection and safeguards for signals intelligence activities

Table of contents

Overview of Swiss data protection and safeguards for signals intelligence activities

1 Introduction

This document has been drafted in support of Switzerland's designation by the Attorney General of the United States as a “qualifying state” pursuant to section 3(f) of Executive Order 14086.

This document describes the key principles of Swiss data protection law (see section 2.1 below) as well as the procedural and enforcement mechanisms in place to support it (see section 2.2 below). It is based on the new legislation which entered into force on 1 September 2023, aimed at strengthening data protection in Switzerland. It also explains the guarantees that apply in relation to data processing by Swiss authorities for criminal law enforcement purposes (see section 3 below). Finally, it provides information on safeguards for signals intelligence activities (see section 4 below).

2 Overview of Swiss data protection

2.1 Swiss data protection framework

On 25 September 2020, the Federal Assembly (Parliament) adopted a new Federal Act on Data Protection (FADP) [1] to replace the Act from 1992 (FADP 1992).

The FADP is complemented by a new Data Protection Ordinance (DPO)[2] and a new Data Protection Certification Ordinance (DPCO)[3], which were adopted by the Federal Council[4] on 31 August 2022[5].

The new legislation strengthens the Swiss data protection framework in several areas, on the one hand to cope with the rapid development of new technologies and on the other hand to take into account developments at the international level, in particular legal developments in the Council of Europe and the European Union in this area.

The FADP, as the previous legal framework, has a broad scope of application, applying to all private operators and federal public authorities. Cantonal and communal public bodies are subject to cantonal data protection rules. All 26 cantons have data protection laws with general principles of data processing, the rights of individuals and oversight by independent cantonal supervisory authorities. Furthermore, the cantons are bound by the fundamental rights guaranteed by the Swiss Federal Constitution (the Constitution). In line with Articles 13 and 36 of the Constitution, any restriction to the fundamental right to privacy must have a legal basis, must be justified by a public interest or the protection of the fundamental rights of others and must be proportionate. Cantonal laws must also be in line with international conventions or treaties concluded by Switzerland, including Convention 108 of the Council of Europe, its additional Protocol 181 (and Convention 108+ once in force[6]), which are directly binding for the cantons[7]. Individuals can appeal up to the Federal Supreme Court if they consider cantonal law

---

1 SR 235.1 - Federal Act of 25 September 2020 on Data Protection (Data Protection Act, FADP) (admin.ch) - please be aware that English is not an official language of the Swiss Confederation and that the English translation of the Swiss legislation is provided for information purposes only and has no legal force.

2 SR 235.11 - Ordinance of 31 August 2022 on Data Protection (Data Protection Ordinance, DPO) (admin.ch).

3 SR 235.13 - Ordinance of 31 August 2022 on Data Protection Certification (DPCO) (admin.ch).

4 The Swiss Government comprises the seven members of the Federal Council. The Federal Council is elected by the United Federal Assembly, that is, by the two parliamentary chambers jointly. For more information, please see Federal Council (admin.ch).

5 The FADP, the DPO and the DPCO entered into force on 1 September 2023.

6 Switzerland ratified the Convention 108+ on 7 September 2023. The Convention 108+ has to date not entered into force yet.

7 The binding effect for the cantons of international treaties in general concluded by the Confederation follows from Article 54 Federal Constitution. This provision establishes the exclusive powers of the Confederation in foreign affairs. Consequently, international treaties concluded by the Confederation are also binding for the cantons which must implement them in their areas of competence.

to infringe federal constitutional or international rules. Furthermore, the FADP codifies the territorial scope of Swiss data protection rules: they apply to events producing effects in Switzerland, even if they take place abroad[8].

The main data protection principles provided under the Swiss data protection framework that were in place in the previous legal framework remain applicable without substantial changes under the FADP. This is the case for the principles of lawfulness[9], purpose limitation[10], proportionality[11], data accuracy[12], data security[13], and accountability. At the same time, the case law and the new legal framework have further strengthened a number of principles (e.g. the principles of data minimisation and storage limitation), and introduced new obligations (e.g. with respect to transparency, data breach notification and accountability).

The principle of proportionality (i.e. requiring that the processing of personal data must be carried out in good faith and in a proportionate manner[14]) has been further clarified in case law as requiring that data must be limited to what is actually and objectively necessary for the defined purposes of processing[15]. The FADP consolidates the principle of proportionality[16] as interpreted in the case law and complements it with the principle of data protection by design and by default[17], explicitly requiring data controllers to ensure (prior to the processing) that the processing of personal data is limited to the minimum necessary to achieve the intended purpose.

The FADP also strengthens the requirement of storage limitation, by introducing a clear obligation to destroy or anonymise data as soon as it is no longer needed for the purpose of processing[18].

Another area that is further strengthened by the FADP concerns transparency of data processing. The FADP requires any controller (i.e. private operators and federal public authorities) to proactively inform the individual[19]. Where data is collected from the data subject, the data controller must at the time when data are obtained, provide the data subject at least with information on the identity and contact details of the controller, the purpose of the processing and, where applicable, the recipients or categories of recipients to whom personal data are transmitted. Where data has not been obtained from the data subject, the controller must provide the data subject with the aforementioned (and additional) information within one month or at the latest when the personal data are first disclosed to another recipient. This obligation concerns both federal administration and private entities processing personal data.

---

8 Article 3 FADP. See also Articles 14 and 15 FADP on the obligations for controllers established outside of Switzerland to, under certain conditions, appoint a representative in Switzerland.

9 See the general principle of lawfulness in Article 6 para. 1 and 2 FADP, as well as Articles 30-31 for private operators and Article 34 for federal public authorities. See also Article 36 FADP with respect to the legal bases for disclosure of personal data by federal public authorities. The general principles of lawfulness, of good faith and of proportionality as codified in Article 6 para. 1 and 2 FADP apply both to the federal authorities and to private operators who process personal data. Article 30 para. 1 FADP specifies that the collection (or further processing) of personal data in violation of these principles constitutes an unlawful violation of privacy. Article 31 establishes the principle that any data processing that violates personal privacy is unlawful unless it is justified by the consent of the data subject, by an overriding private or public interest, or by law.

10 Article 6 para. 3 FADP.

11 Article 6 para. 2 FADP.

12 Article 6 para. 5 FADP.

13 Article 8 FADP.

14 Article 4 para. 2 FADP 1992.

15 Decision A-3144/2008 of 27 May 2009 of the Federal Administrative Court.

16 Article 6 para. 2 FADP.

17 Article 7 FADP.

18 Article 6 para. 4 FADP.

19 Article 19 FADP.

Where data are transferred abroad, data subjects must be informed about the country of destination and the safeguards that are put in place.

With respect to data security, the FADP introduces a requirement for controllers to notify data breaches as soon as possible: (1) to the federal data protection authority (Federal Data Protection and Information Commissioner, FDPIC), where they are likely to result in a high risk to the data subject's personality or fundamental rights; and, (2) to the data subject, where necessary for his or her protection or when required by the FDPIC[20]. Moreover, the requirements regarding data security have been considerably extended in the DPO[21].

In addition, the FADP and the DPO[22] modernise existing accountability requirements (e.g. to maintain a record of processing, issue a privacy policy and register certain types of processing with the FDPIC, e.g. in case of large scale processing of sensitive data[23]). The FADP requires controllers to implement the principles of data protection by design and by default[24], keep a record of processing activities[25], conduct a data protection impact assessment for data processing likely to result in a high risk to the data subject's personality or fundamental rights[26], and, in certain circumstances, consult the FDPIC prior to data processing (e.g. if an impact assessment shows that the processing would involve high risks for the concerned individuals)[27]. Moreover, the FADP foresees the appointment of data protection officers (as possibility for private operators and as obligation for federal public authorities)[28], and provides for the possibility to adhere to sectoral codes of conduct[29] and participate in certification schemes[30].

In addition to the strengthening of data protection principles and obligations, the protections for special categories of data have been reinforced. The previous legal framework already offered additional protection for personal data on religious, ideological, political or trade union-related views or activities, health data, data related to intimate sphere, racial origin, social aid measures and administrative and criminal proceedings and sanctions. The FAPD, similarly to EU data protection law, has added to the list also data on ethnic origin, genetic data and biometric data which uniquely identifies a natural person[31].

With respect to the rights of data subjects, the Swiss data protection framework continues to provide for a right of access, correction and erasure[32], as well as a right to object[33]. At the same time the FADP has reinforced and modernised several rights. This is particularly the case for the right of access: under the FADP, controllers are required to provide additional information in response to an access request (including the identity and contact details of the controller,

---

20 Article 24 FADP.

21 Articles 1-6 DPO.

22 See Articles 1-6 and 42 DPO.

23 See Articles 7, 10a and 11a FADP 1992, as well as Articles 3-4, 8-11, 16, 18, 20-21 and 28 DPO of 1993.

24 Article 7 FADP.

25 Article 12 FADP.

26 Article 22 FADP.

27 Article 23 FADP.

28 Article 10 FADP.

29 Article 11 FADP.

30 Article 13 FADP.

31 Article 5 letter c FADP.

32 Article 32 para. 2 letter c (for private operators) and Article 41 para. 1 FADP.

33 Articles 32 para. 2 letters a-b and 41 para. 1 letter a FADP,. With respect to public authorities, Art. 37 FADP provides individuals with an additional specific right to object to the disclosure of their data.

the retention period and the recipients or categories of recipients to whom personal data are disclosed) and data subjects must be provided with the information necessary to enable them to assert their rights and to ensure the transparency of the processing[34]. With respect to the right of correction, the FADP limits the possibility for controllers to refuse to rectify inaccurate data to situations where a statutory obligation prohibits the rectification or the personal data is processed for archiving purposes in the public interest[35].

Moreover, new rights have been introduced under the FADP. This includes rules for automated individual decision-making, in particular a duty to inform the data subject about decisions taken exclusively on the basis of automated processing that produce legal effects or similarly significantly affect the individual[36], to give the individual the opportunity to make known his or her views upon request and to ensure review by a natural person upon request of the data subject. Moreover, the FADP provides for a right to data portability, i.e. a right to receive a copy of personal data processed by automated means in a commonly used format, or to have such personal data transferred to another controller[37].

Finally, the rules on international transfers of personal data have been reinforced. As a general rule, personal data may only be transferred if the data is subject to adequate protections in the country of destination[38]. Under the FADP 1992, the FDPIC had developed an indicative list of states that provide an adequate level of data protection, but it remained the responsibility of the data exporter to assess whether and ensure that data will be adequately protected in another state. The FADP introduces a change of competence: the Federal Council is in charge of deciding whether a state or international organisation offers an adequate level of protection, on which data exporters can rely to transfer data without the need to carry out their own assessment or put in place specific safeguards[39]. The criteria to be taken into account for the evaluation of the adequacy of the level of protection are listed in Article 8 of the DPO. These criteria are the following: a) the international obligations of the State or international body, in particular in relation to data protection; b) whether it respects the rule of law and human rights; c) the legislation applicable, in particular to data protection, its implementation and the relevant case law; d) that data subjects' rights and redress are effectively guaranteed; e) the effective functioning of one or more independent authorities in the State concerned that are responsible for data protection or to which an international body is accountable and that have sufficient powers and responsibilities. A list of states and territories adequately protecting personal data will be published in Annex 1 to the DPO.

If a state is not recognised as providing an adequate level of data protection, personal data may only be transferred to that state if sufficient safeguards are put in place by the data exporter and importer to ensure an adequate level of protection (e.g. by means of contractual clauses or binding corporate rules[40]) or on the basis of specific statutory grounds (e.g. if the individual has consented to the transfer, the transfer is necessary in a specific case to safeguard an

---

[34] Article 25 of the FADP. The relevant information must be provided free of charge and, in principle, within 30 days of the request.

[35] Article 32 para. 1 FADP.

[36] Article 21 FADP.

[37] Article 28 FADP and Art. 20-22 DPO.

[38] Article 16 para. 1 FADP.

[39] Article 16 para. 1 FADP.

[40] See Article 16 para. 2 letters b and e FADP.

overriding public interest, the transfer is necessary in a specific case to protect the life of the data subject, etc.[41]).

In general, the FADP also applies to the Federal Intelligence Service (FIS) unless there is a specific provision in the Intelligence Service Act (IntelSA)[42] (see section 4 below).

2.2 Oversight and redress

The independent body in charge of overseeing compliance with the data protection rules by private operators and federal public authorities in general is the FDPIC[43] (regarding oversight and redress in relation with access to data by Swiss public authorities for national security purposes, please refer to 4.2.5 and 4.2.6 below). The FDPIC's tasks include advising and assisting controllers on data protection matters, providing opinions on draft legislation that is relevant to data protection, cooperating with domestic and foreign data protection authorities and raising public awareness on data protection[44]. Similarly, the supervision of cantonal and communal public authorities is carried out by independent cantonal and/or communal data protection authorities[45].

In terms of powers, the FADP provides that the FDPIC may initiate an investigation on its own initiative or upon request of a third party with respect to both private operators and public authorities[46]. In carrying out its investigations, the FDPIC has access to any relevant information[47]; this includes access to sensitive national security information[48]. If the data subject has filed a report, the FDPIC shall inform him or her about the steps taken in response and the result of any investigation[49]. The FDPIC's investigatory and enforcement powers have been strengthened by the FADP, which provides it with the power to compel access to premises and documents[50] and adopt binding decisions with respect to both private operators and public authorities (including intelligence agencies), including to modify, suspend or terminate processing or destroy personal data[51].

In addition, the Swiss legal framework imposes criminal fines for certain violations of data protection rules by private operators. The FADP expands the list of violations for which fines can be imposed (adding inter alia intentional infringements of the obligations to inform data subjects and cooperate with the FDPIC[52], violating the duty of care[53], and failing to comply with

---

41 See Article 17 FADP.

42 SR 121 - Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, IntelSA) (admin.ch).

43 The head of the FDPIC is appointed for a term of four years by the United Federal Assembly (Parliament), which may be renewed twice (see Article 44 FADP). The FADP provides that the head of the FDPIC exercises its duties independently, does not receive instructions from any authority or third party, has its own budget and appoints its own staff (see Article 43 para. 4 and 5 FADP). The head of the FDPIC may not have any other occupation, unless specifically authorised by the Federal Assembly, provided such other occupation does not compromise his/her independence and standing (see Articles 46-47 FADP). The United Federal Assembly may remove the head of the FDPIC from office before the end of the term of office if he or she: a) has wilfully or through gross negligence committed a serious violation of his or her official duties; or b) has permanently lost the capacity to carry out his or her official duties (see Art. 44 FADP).

44 See Article 58 FADP.

45 All cantonal data protection laws prescribe the election of independent data protection authorities and provide that these authorities shall be independent in their position and in the performance of their duties.

46 Article 49 FADP.

47 Article 49 para. 3 and 50 para. 1 letter a FADP.

48 See Article 63 para. 3 and 64 IntelSA.

49 Article 49 para. 4 FADP.

50 Article 50 FADP.

51 Article 51 FADP.

52 Article 60 FADP.

53 Article 61 FADP.

a decision of the FDPIC[54]) and imposes a maximum amount of CHF 250'000. While such fines are in principle imposed on individuals, the FADP also foresees the possibility of fining a company, where determining who in the organisation is responsible for the infringement would require disproportionate investigative efforts[55]. Other Swiss laws, including the Swiss Criminal Code (SCC)[56], contain further criminal sanctions for violations of the privacy of individuals as well (e.g. obtaining personal data without authorisation)[57].

As regards the possibility for individuals to obtain redress, different avenues are available in the Swiss system. In particular, individuals can obtain judicial redress before the civil courts (against private operators) and under the Administrative Procedure Act[58] (against public authorities), including by directly enforcing their individual rights[59], obtaining the termination of unlawful processing[60], or claiming compensation for damages[61].

The FDPIC regularly engages “upstream” with data controllers and data processors by advising on data protection matters while projects and IT systems are being developed. This includes working with private operators (e.g. through impact assessments) as well as federal public bodies (e.g. in the context of digitalisation within the federal administration). The FDPIC also plays an active role by advising on data protection issues during the legislative process.

The FDPIC also carries out investigations[62] (e.g. into a data breach at a telecommunications provider[63], the use of GPS data by a music streaming service[64], the processing of data by a dating application[65], data practices of insurance companies and financial institutions[66], etc.).

Finally, the FDPIC also issues guidance documents, e.g. on data subject rights[67], cross-border data flows[68], the processing of data for marketing purposes[69] and technical and organisational measures[70]. The FDPIC also provides assistance to individuals by answering queries, running a phone helpline and offering model letters which can be used by data subjects to exercise their rights.

---

54 Article 63 FADP.

55 Article 64 FADP.

56 SR 311.0 - Swiss Criminal Code of 21 December 1937 (admin.ch).

57 See e.g. Articles 143 and 179novies of the Swiss Criminal Code.

58 SR 172.021 - Federal Act of 20 December 1968 on Administrative Procedure (Administrative Procedure Act, APA).

59 See Article 32 (with respect to private operators) and 41 (with respect to federal public authorities) FADP.

60 E.g. pursuant to Article 28a of the Swiss Civil Code (SR 210 - Swiss Civil Code of 10 December 1907 (admin.ch)).

61 Pursuant to Article 41 and 49 of the Swiss Code of Obligations (SR 220 - Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) (admin.ch)) and the Federal Act on the Liability of the Confederation, Members of its Authorities and Officials (RS 170.32 - Loi fédérale du 14 mars 1958 sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (Loi sur la responsabilité, LRCF) (admin.ch) (not available in English)).

62 See Final reports and recommendations Data Protection (admin.ch) as well as Court proceedings (admin.ch).

63 See FDPIC's 27th Activity Report 2019/20: German p. 20 ; French p. 20.

64 See FDPIC's 27th Activity Report 2019/20, p 22.

65 See FDPIC's 28th Activity Report 2020/21: German p. 20; French p. 20 and 29th Activity Report 2021/22 : German p. 17 ; French p. 17. The final report should be published soon on the FDPIC's website.

66 https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/aDSG/empfehlungen-ds/Empfehlung%20Helsana.pdf.download.pdf/Empfehlung%20Helsana.pdf.

67 Right to information (admin.ch).

68 Cross-border transfer of personal data (admin.ch).

69 Advertising & marketing (admin.ch).

70 Internet & Technology (admin.ch).

3 Access by Swiss public authorities for criminal law enforcement purposes

3.1 Legal bases and applicable safeguards

Any federal authority whose mandate involves the processing of personal data is in principle subject to the provisions of the FADP. This concerns also national security and criminal law enforcement, with the exception of criminal proceedings, governed by data protection provisions in the Criminal Procedure Code (CrimPC) [71].

The general requirement, set out in Art. 34 para. 1 and 36 of the FADP is that federal bodies may in principle only process personal data if there is a legal basis for doing so. They may only process sensitive personal data or use profiling if a formal legal basis expressly provides so or by way of listed exceptions.

The CrimPC establishes rules governing privacy in criminal proceedings[72]. They apply to both federal and cantonal criminal justice authorities. General data protection rules applicable to criminal proceedings and regarding the activities of law enforcement authorities and in particular the police in this context, are provided in Art. 95 to 99 CrimPC. In addition to that, data collected by these authorities become part of the general file under the control of the public prosecutor's office. Therefore, Art. 100 to 103 CrimPC, which regulate the management, inspection and retention of case files, are applicable as well. Finally, Art. 349*a* to 362 of the SCC lay down requirements to the processing of personal data in the context of international administrative police cooperation, which, with a few exceptions, apply to both the federal and cantonal law enforcement authorities.

As long as proceedings are pending, the parties and the other participants in the proceedings have, in accordance with their right to inspect case documents, the right to information on personal data relating to them that has been processed (Art. 97 CrimPC). Where personal data proves to be incorrect, the relevant criminal justice authorities must correct it immediately. They must immediately notify the authority which transmitted or made available such data to them or to which they disclosed the data of the corrections (Art. 98 CrimPC).

The CrimPC requires a two-step approach when government agencies use, in order to prevent or detect serious crime, covert surveillance measures.[73] In cases of covert surveillance measures, an order from the public prosecutor to carry out such surveillance must be authorised by the Compulsory Measures Court[74] (Art. 274 or Art. 289 CrimPC with regard to undercover investigations). Given that the CrimPC is technologically neutral, these provisions also apply to the surveillance of electronic information (e.g. communications in the internet, e-mails) insofar as there is communication involved and not just storage. The authorisation procedure requires the public prosecutor to inform the Compulsory Measures Court within 24 hours on the surveillance order (i.e. the court takes a decision when the surveillance is already ongoing, and not only in emergency situations). The Court must decide within 5 days either to grant or refuse authorisation. The Court may grant authorisation subject to a time limit or other conditions, or

---

[71] https://www.fedlex.admin.ch/eli/cc/2010/267/fr (not available in English).

[72] Since the CrimPC has its own data protection provisions, the criminal proceedings have been excluded from the FADP (Art. 2 para. 3 FADP) in order to avoid legal uncertainty regarding the applicable data protection regulations. The applicable procedural law (Art. 95 ff. CrimPC) ensures the protection of privacy and of the rights of the persons involved and guarantees a level of protection equivalent to the FADP.

[73] See Art. 269-298 CrimPC. The surveillance of post or telecommunications and the procedure therefor is further governed by the Federal Act on the Surveillance of Post and Telecommunications (SPTA) of 18 March 2016 (SR 780.1 - Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) (admin.ch)).

[74] The Compulsory Measures Court is a court responsible for ordering the accused's remand or preventive detention and, where the SCC so provides, for ordering or approving additional compulsory measures. Compulsory measures are procedural acts carried out by the criminal justice authorities that restrict the fundamental rights of the persons concerned and which serve to secure evidence, to ensure that persons attend the proceedings and to guarantee the execution of the final judgment.

request further information or investigations. Additional requirements are: a strong suspicion that a specific, qualified offence has been committed, the offence must be of gravity that justifies surveillance and the measures taken must be proportionate (e.g. surveillance is a proportionate measure when investigative activities carried out so far have been unsuccessful, or the enquiries would otherwise have no prospect of success or would be made unreasonably complicated, Art. 269 para. 1 letter c CrimPC). The public prosecutor must stop surveillance immediately if the requirements are no longer fulfilled or the authorisation or its extension is refused (Art. 275 CrimPC). Records of authorised surveillance operations that are not required for criminal proceedings must be stored separately from the case documents and destroyed immediately on conclusion of the proceedings (Art. 276 CrimPC). Records of surveillance operations that have not been approved by the Court have to be destroyed immediately and information gained through such surveillance must not be used (Art. 277 CrimPC).

The surveillance of post and telecommunications (including electronic communications) is subject to specific information obligations[75] in the CrimPC, which take precedence over the general information obligation in Art. 95 para. 2 CrimPC. The supervised person is informed about the surveillance in hindsight and can appeal against it. If, in exceptional cases, overriding public or private interests stand in the way of this notification and the findings are not used as evidence, the notification can only be postponed or omitted altogether with the approval of the Compulsory Measures Court (Art. 279 para. 2 CrimPC).

Persons whose telecommunications connection, electronic connection or postal address have been under surveillance or who have used a connection or postal address that has been under surveillance may file an objection to the competent authorities according to article 20 and 279 para. 3 CrimPC. On the federal level, objections can be filed to the Federal Criminal Court[76].

3.2 Oversight and redress

The FDPIC supervises compliance by federal bodies (Art. 4 para. 1 FADP). The FDPIC supervisory powers extend also to the processing of personal data by federal agencies for the purposes of criminal law enforcement with the exception of pending criminal proceedings, where his supervision would compromise the separation of powers and independence of the judiciary.

As regards individual redress in the law enforcement sector, criminal procedural remedies are available against legal violations. Decisions rendered by criminal law enforcement authorities may be appealed to the federal courts in accordance with the applicable rules of procedure. If the person concerned intends to claim a data protection violation in criminal proceedings (as well as mutual assistance proceedings), he or she must do so within the framework of these proceedings and follow the legal channels provided for this purpose.

Data subjects may file an objection to any decision or ruling by the police, the public prosecutor, courts of first instance and the Compulsory Measures Courts (Art. 393 CrimPC). This objection can be filed e.g. against the disclosure of personal data, the denial of the right of information or the rejection of the request for correction of data by the responsible law enforcement authorities in the context of pending criminal proceedings. The right to file an objection is subsidiary[77] to the right of appeal under Art. 398 CrimPC. An objection against decisions issued in writing or orally must be filed within 10 days in writing and with a statement of grounds with the objections authority. The period for filing the objection begins on receipt of the notice. According to Art.

---

[75] Similar specific information obligations can be found in Art. 283 (observation) and Art. 298 (undercover investigations) CrimPC.

[76] Art. 37 para. 1 of the Federal Act on the Organization of Federal Criminal Authorities (https://www.fedlex.admin.ch/eli/cc/2010/444/fr).

[77] Art. 394(a) CrimPC.

431 para. 1 CrimPC, the criminal justice authority must award the accused person reasonable compensation and reparation, if compulsory measures have been applied unlawfully.

After exhausting possibilities of redress at national level, an individual may bring the case to the European Court of Human Rights (ECtHR).

4 Access by Swiss public authorities for national security purposes

4.1 Introduction

The FIS is a Swiss security policy instrument with a mandate that is clearly defined in legal terms. The FIS is concerned with early perception and prevention of terrorism, violent extremism, espionage, proliferation of weapons of mass destruction and their delivery system technology as well as cyberattacks against critical infrastructure. Furthermore, the FIS obtains information relevant to security policy abroad and evaluates it. In this way it contributes decisively towards comprehensive assessment of the threat situation. At the federal level the FIS primarily serves the Federal Council, departments of the federal administration and the military command. The FIS also helps the cantons maintain inner security and supports federal law enforcement authorities. The preventive activity of the FIS must be clearly distinguished from the repressive role of law enforcement authorities. The FIS is not a law enforcement authority. Its core tasks are prevention and situation assessment on behalf of the executive branch.

On 25 September 2015, the Federal Assembly of the Swiss Confederation decreedthe IntelSA. The Swiss electorate voted in favour of the IntelSA on 25 September 2016 and it finally came into force on 1 September 2017, together with the Ordinance on the Federal Intelligence Service (FISO)[78], the Ordinance on the FIS Information and Storage Systems (ISSO-FIS)[79], and the Ordinance on the Supervision of Intelligence Activities (OSIA)[80]. The Act reformulates the Federal Intelligence Service's responsibilities for providing a comprehensive situation assessment. It also allows for the protection of national interests of strategic importance, such as critical infrastructure and the Swiss financial and industrial sectors.

The state must exercise the utmost restraint with regard to any intrusion on personal privacy. The information gathering resources introduced by the IntelSA are to be used only after prior approval by the Federal Administrative Court[81] and clearance by the Head of the Federal Department of Defence, Civil Protection and Sport (DDPS)[82], after consulting the Head of the Federal Department of Foreign Affairs (FDFA) and the Head of the Federal Justice and Police Department (FDJP).

Moreover, the FIS is subject to much stricter supervision. All FIS activities are subject to continuous checks. The FIS is supervised by an independent supervisory authority, the Federal Council, Parliament and the Federal Administration.

In addition, Switzerland respects the principles enshrined by the ECtHR on government access for national security purposes, notably the requirement that each interference with the right to privacy must be provided for by law, the requirement that each interference must pursue a

---

78 https://www.fedlex.admin.ch/eli/cc/2017/495/fr (not available in English)

79 RS 121.2 - Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC) (admin.ch) (not available in English)

80 https://www.fedlex.admin.ch/eli/cc/2017/497/fr (not available in English)

81 The judges of the Federal Administrative Court are elected by the United Federal Assembly of Switzerland for a term of six years, with reelections possible. Though according to Art. 5 of the Federal Act on the Federal Administrative Court anyone entitled to vote in federal matters is eligible for election, comprehensive legal training is an essential requirement in practice and eminent lawyers are generally elected as judges. According to Art. 30 of the Swiss Federal Constitution, the courts shall be legally constituted, competent, independent and impartial. Furthermore, Art. 191c of the Swiss Federal Constitution states that the judicial authorities are independent in the exercise of their judicial powers and are bound only by the law. Judges may be removed from the Federal Administrative Court by the United Federal Assembly of Switzerland only if a judge (i) has willfully or through gross negligence committed a serious violation of his or her official duties or (ii) has permanently lost the capacity to carry out his or her official duties.

82 The FIS is administratively located within the DDPS and its director personally reports to the Head of the DDPS.

legitimate aim, the necessity and proportionality of the measure as well as the need for minimum safeguards to prevent abuse.

4.2 Safeguards for signals intelligence activities

This section aims to discuss protection of U.S. person's personal data transferred to Switzerland by appropriate safeguards regarding signals intelligence activities.

4.2.1 Overview of signals intelligence activities and authorisations under Swiss law

a. Government agencies with responsibility to collect, process, or share information for foreign intelligence and national security purposes

The FIS is assigned responsibility to collect, process or share information for signals intelligence activities.

Intelligence measures are also carried out by the Swiss Armed Forces. Personal data processed by the Army Intelligence Service (MIS) are regulated in the Military Act[83] and the related ordinance[84]. However, the tasks of the MIS are limited to the military area of competence.

b. Laws authorising signals intelligence activities

The activities of the FIS are authorized by the IntelSA. Where the IntelSA does not provide specific data protection provisions, the FADP and more generally the constitutional principles applicable for public authorities[85] are relevant for data processing[86] (see also 4.1 and 4.2.1a above).

Activities	Legal authorisation
Information gathering from public sources of information	Art. 13 IntelSA - information gathering measures not requiring the double authorisation procedure
Information gathering from observation of public in generally accessible locations	Art. 14 IntelSA - information gathering measures not requiring the double authorisation procedure
Information gathering from human sources	Art. 15 IntelSA - information gathering measures not requiring the double authorisation procedure
Alerts on persons and property	Art. 16 IntelSA - information gathering measures not requiring the double authorisation procedure

[83] See Art. 99 of the Military Act. https://www.fedlex.admin.ch/eli/cc/1995/4093_4093_4093/fr (not available in English).

[84] Ordinance on the Army Intelligence Service. RS 510.291 - Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée (OSRA) (admin.ch) (not available in English).

[85] Art. 5 Swiss Constitution stipulating that all administrative action must comply with the principles of lawfulness, proportionality and of good faith.

[86] According to the principles of legality (Article 6(1)) and good faith (Article 6(2)), the FIS and the ACEM may only process personal data if and to the extent that they are authorized by law. The principle of proportionality (Article 6(2)) obliges the ACEM and the FIS to process personal data only to the extent that is suitable to achieve the required purpose and to process only data that is necessary for this purpose. In addition, the purpose of the data processing must be proportionate to the interference with fundamental rights. This latter criterion requires a balancing of the private interest of the person concerned and the public interest in processing personal data. The principle of proportionality moreover stipulates that personal data should only be retained for as long as is appropriate and necessary to achieve the legitimate purpose. The principle of purpose limitation (Article 6(3)) obliges the FIS and the ACEM to process personal data only within their competences and for the legally prescribed purpose. Finally, pursuant to article 8 FADP, the FIS and the ACEM must apply all necessary technical and organizational measures in order to ensure data security and integrity.

Secret surveillance of post and telecommunications, use of special technical devices, use of localisation devices to establish the location and the movements of persons or objects, use of monitoring devices, intrusion into computer systems and computer networks, search of premises, vehicles or storage facilities	Art. 26 IntelSA - information gathering measures requiring the double authorisation procedure
Intrusion into computer systems and computer networks abroad	Art. 37 IntelSA - information gathering measures deployed on computer systems outside Switzerland, requiring authorization from the Federal Council or three of its members
The Confederation may operate a service for recording electro-magnetic emissions from telecommunications systems located abroad (radio communications intelligence)[87].	Art. 38 IntelSA - radio communications intelligence not requiring the double authorisation procedure
Cable communications intelligence mandates	Art. 40 IntelSA - information gathering measures requiring the double authorisation procedure

The activities of the MIS are authorized by the Military Act.

c. Types of intelligence data access authorised and legal bases

Provisions on data processing for national security purposes can be found in particular in Art. 44 ff. of the IntelSA. In addition to empowering the FIS to process data, these provisions also set out various processing principles (including lawfulness, proportionality and quality assurance). The FADP is applicable to intelligence activities insofar as the IntelSA does not provide specific data protection provisions. As an example, for what concerns retention and storage, the IntelSA and the ISSO-FIS provide specific provisions hence there is no need to refer to the FADP. On the contrary, the IntelSA does not provide specific provisions on recording of processing activities, therefore the provisions of the FADP (see Art. 12 FADP) in this respect are applicable.

Data processing by the MIS is governed by the Military Act and the related ordinance (see 4.2.1a above).

In addition, the Federal Act on Measures to Protect National Security of Switzerland[88] contains some provisions on data processing (preventive police measures in relation with threats to internal security).

---

[87] The service operator is subject to Swiss law. Furthermore, Art. 4 of the Ordinance on electronic warfare and radio exploration (RS 510.292 - Ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio (OGE) (admin.ch) - not available in English) provides that all results of radio communications, including communications data and metadata, will be destroyed 5 years after terminating the exploration mandate.

[88] https://www.fedlex.admin.ch/eli/cc/1998/1546_1546_1546/fr (not available in English)

i. Legal authorisations applying to interception of electronic communications, access to stored data held by private companies

Information gathering measures that are potentially the most damaging to fundamental rights such as the use of special technical devices to monitor telecommunications or to record transmissions or the intrusion into computer systems and computer networks are subject to a double authorisation procedure according to Art. 26 ff. IntelSA[89] (as mentioned above).

First, an application must be submitted to the Federal Administrative Court, which examines it from a legal point of view; with reference to the principles governing information gathering (see Art. 5 IntelSA), the Federal Administrative Court will notably examine whether the information gathering measure is most suitable and necessary for achieving a specific information gathering objective and causes the least interference with the fundamental rights of the persons concerned. This implies that the Federal Administrative Court examines the proportionality of the information gathering measure as well as whether the categories of key words are necessary for the fulfillment of the order of the FIS in question.

In this respect, Art. 29 IntelSA specifies the authorization procedure and the factual and legal elements which the FIS must provide to the Federal Administrative Court[90]; the Federal Administrative Court has full cognitive power and sets high standards for the statement of grounds. After the Federal Administrative Court has given its approval, the measure must be approved by the Head of the DDPS, who must consult the Head of the FDFA and the Head of the FDJP. Cases of particular importance may be submitted to the Federal Council.

ii. Legal authorisations applying to acquisition of the content of communications, traffic information, subscriber information

See 4.2.1.c.i. above.

iii. Legal authorisations applying to access through compulsory orders issued to private companies to disclose data, and to direct access to data without the knowledge of the data holder

Art. 25 IntelSA regulates special duties of private individuals to provide information: insofar as necessary to identify, prevent or repel a specific threat to internal or external security, 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. Hence there is a legal obligation for the concerned natural or legal person to provide information. According to Art. 83 IntelSA rulings based on the IntelSA issued by the FIS may be contested by appeal to the Federal Administrative Court; such an appeal does not have the effect of suspending the ruling. 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[91].

The FIS may also obtain information in accordance with Art. 15 of the Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) [92] to fulfill its tasks under the IntelSA. According to Art. 3 SPTA, a service for the surveillance of post and

---

89 Under Art. 26 ff. IntelSA, the same procedure applies to the different information gathering measures requiring authorisation independently from the types of data sought.

90 As per Art. 29 para. 1 letter b IntelSA, the application must notably include data pertaining to persons or organisations affected by the measure. A measure not targeting specific persons would thus be rejected by the Federal Administrative Court.

91 https://www.fedlex.admin.ch/eli/cc/2006/218/fr (not available in English).

92 SR 780.1 - Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) (admin.ch)

telecommunications, the Post and Telecommunications Surveillance Service (PTSS), is operated under Art. 269 CrimPC; the PTSS is administratively assigned to the FDJP. The PTSS shall perform its tasks[93] autonomously and is not subject to instructions. According to Art. 15 SPTA, this service shall provide the authorities cited in this provision with information on the data referred to in Articles 21 (information on telecommunications services) and 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), on request and only for specific purposes: in the case of the FIS: for the purpose of fulfilling tasks under the IntelSA[94]. The data that may be obtained by the PTSS from telecommunications providers for the FIS is limited to basic subscriber information, such as the identity of the person registered to a phone number or electronic communications account.

Furthermore, based on Art. 28 IntelSA[95], the FIS may order an information gathering measure requiring authorisation in relation to a third party if there is reason to believe that this person is using premises, vehicles or storage facilities belonging to the third party o the latter's postal addresses, telecommunication connection points, computer systems or computer networks in order to transmit, receive or store information.

According to Art. 33 IntelSA, 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. It may postpone or dispense with giving notification in the following cases: a. if 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.

According to Art. 26 ff. IntelSA, information gathering measures that are potentially the most damaging to fundamental rights, such as direct access to data without the knowledge of the data holder, are subject to a double authorisation procedure as described under i. above.

In any case the FIS is legally bound to choose the information gathering measure that is most suitable and necessary for achieving a specific information gathering objective and causes the least interference with the fundamental rights of the persons concerned (see Art. 5 IntelSA).

iv. Legal authorisations applying to acquisition through targeting specific persons or communications accounts, and to non-individualized/programmatic surveillance

The IntelSA authorizes cable communications intelligence to protect important national interests not only on a reactive but also on a preventive basis. The FIS may under certain conditions instruct the service carrying out the communications intelligence to record cross-border signals from cable-based networks (Art. 39 IntelSA)[96]. Cable communications intelligence mandates require the same double authorisation as described above (Art. 40 IntelSA). If the FIS intends to issue a mandate for cable communications intelligence, it shall file an application with the Federal Administrative Court that includes: (a) a description of the mandate to be issued to the service carrying out the communications intelligence; (b) the

---

93 The tasks of the PTSS are stipulated in Articles 15-18 SPTA.

94 The PTSS remit is all communications involving persons on the Swiss territory. The PTSS is only competent to perform a formal verification of surveillance orders (Art. 16 letters a and b SPTA). The substantive verification of surveillance orders is performed by the Federal Administrative Court in the case of the IntelSA as a double authorisation (including judicial authorisation) is required for surveillances of post and telecommunications (Art. 26 para. 1 letter a IntelSA).

95 The measures under Art. 28 IntelSA are the same as in Art. 26 IntelSA, including access to communications held by private providers.

96 According to Art. 39 IntelSA, the FIS may instruct the service carrying out the communications intelligence to record cross-border signals from cable-based networks in order to gather information about events outside Switzerland that are of significance to security (see Art. 6 para. 1 let. b IntelSA) and to safeguard additional important national interests in accordance with Art. 3 IntelSA. Therefore, if both communicants are located in Switzerland, the recorded signals may not be used.

reasons why the operation is necessary; (c) details of the categories of search parameters[97]; (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 on when the operation will start and finish. 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. 41 IntelSA). The double authorisation procedure described under i. above also applies to the issuance of a mandate for cable communications intelligence by the FIS. The Federal Administrative Court has full cognitive power when deciding on the approval of surveillance measures and therefore assesses also whether the measures comply with the general constitutional and data protection principles.

It is noteworthy that the Federal Supreme Court rejected a decision of the Federal Administrative Court in its Judgment 1C_377/2019 and confirmed the right of everyone to challenge the interceptions over cables and/or airways by the FIS (the claimants proceeded to challenge the surveillance by means of interceptions over cables and/or airways)[98]. The right of claimants to substantive examination of their applications derives from Article 13 of the European Convention on Human Rights (ECHR). At a minimum, the provision ensures that a person who reasonably argues that he or she is a victim of an ECHR violation can file an effective complaint with a national body. The ECtHR has emphasized in its case law the central importance of domestic legal protection in the review of secret mass surveillance systems. It must therefore be possible for the system as a whole to be reviewed by at least one independent authority before those affected can bring an individual complaint to the ECtHR. With its judgment 1C_377/2019 the Federal Supreme Court takes into account, respects and implements this constant jurisprudence of the ECtHR. The Federal Supreme Court consequently referred the case back to the Federal Administrative Court, instructing it to examine whether the presumed processing of data in the current radio and cable intelligence program violates the fundamental rights of the plaintiff under the Federal Constitution and the ECHR, and if so, to decide the legal consequences. The case is pending before the Federal Administrative Court.

d. Legal authorisations and responsibilities applying to signals intelligence activities conducted within the territory of Switzerland, and outside the territory of Switzerland

The IntelSA distinguishes between information gathering measures within the territory of Switzerland not requiring authorisation (Art. 13 ff.) and requiring authorisation (Art. 26 ff.). These provisions also apply if information about events outside Switzerland is procured domestically (Art. 36 para. 2)[99].

Information gathering about events outside Switzerland, which also include radio and cable communications intelligence, are regulated by Art. 36 ff. IntelSA. According to Art. 36 para. 1 IntelSA, the FIS may covertly gather information about events outside Switzerland, be it by procuring information in Switzerland or outside the territory of Switzerland. Art. 36 para. 3 and 4 IntelSA indicates the conditions under which such surveillance activities can be conducted, i.e. 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. The FIS shall also document in-

---

[97] The FIS proposes the search parameters to the Federal Administrative Court and the Court reviews and approves or rejects them. A certain degree of specificity is required for the Federal Administrative Court to be able to make a decision.

[98] 1C_377/2019 01.12.2020 - Tribunal fédéral (bger.ch) (not available in English). The applicant, a private Swiss association “Digitale Gesellschaft”, established for the protection of citizens and consumers, claimed that the operation of radio and cable surveillance by the FIS and other agencies, in particular the CEO, violates its fundamental rights such as the right to and protection of privacy, protection against the misuse of personal data and to informational self-determination, freedom of assembly and the presumption of innocence.

[99] For the sake of clarity, this means that for the types of collection measures in Section 6 of the IntelSA (of which Art. 36 is part), the provisions of Section 6 apply in addition to the provisions of Section 4 (i.e. Art. 26 ff.).

formation gathering about events outside Switzerland for the attention of the supervision and control bodies.

4.2.2 Legitimate objectives for collecting signals intelligence

a. Objectives based on which intelligence agencies are authorised to collect data through signals intelligence

The FIS collect data in connection with national security and such collection is subject to specific requirements under the IntelSA. According to Art. 6, the FIS can gather and process information for the following purposes: early recognition and prevention of threats to internal or external security (e.g., terrorism, espionage, proliferation of nuclear, biological or chemical weapons, violent extremism); to identify, observe and assess events outside Switzerland that are of security-policy significance; or to safeguard Switzerland's capacity to act. Furthermore, and according to Art. 2, the aims of the IntelSA are: 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; c. to support Switzerland's capacity to act; d. to contribute towards safeguarding international security interests.

It should be noted that Art. 6 para. 1 letter a IntelSA describes the general tasks assigned to FIS and the powers with respect to data processing, whilst Art. 19 para. 2 elaborates on the threats described in Art. 6 para. 1 to justify the providing of information from public authorities to the FIS. The threat categories are the same in both articles, so that Art. 27 para. 1 referring to Art. 19 para. 2 does not have any material distinction.

b. List of legitimate objectives for signals intelligence to be amended unilaterally by the Federal Council

According to Art. 3 IntelSA, 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.

c. Prohibited objectives and important principles to be respected

According to Art. 5 para. 5 IntelSA, the FIS may not gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland with the exception of the specific circumstances described in Art. 5 para. 6-8.

In any case, information gathering must respect important principles: in each case, the FIS 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 (see Art. 5 para. 3 IntelSA).

The IntelSA governs the safeguarding of Switzerland's essential interests in the field of security policy. The objectives are listed in Art. 2 IntelSA. Moreover, and as explained under 4.2.2.b. above, further important national interests can be safeguarded in the event of a serious and immediate threat (Art. 3 IntelSA): the protection of Switzerland as a location for employment, business and finance is among these objectives. The Dispatch of the Federal Council on the IntelSA[100] illustrates this objective by indicating that this would be the case e.g. in the event of pressure directed against specific economic sectors of national importance. This would however not authorise FIS to afford a competitive advantage to Swiss companies and Swiss business sectors commercially. Furthermore Art. 23 FISO protects professional secrets and

[100] https://www.fedlex.admin.ch/eli/fga/2014/407/fr (not available in English)

stipulates that it must be ensured that the FIS does not come into possession of information related to a professional secret and unrelated to the reason for the surveillance.

4.2.3 Collection of signals intelligence

a. Prior independent approval of signals intelligence collection

Please refer to 4.2.1.c.i. and iii. as well as 4.2.1.d. above[101].

b. Attributes of independence of approving authorities

The Federal Administrative Court involved in the double authorisation procedure is, as judicial authority, fully independent and therefore outside of any executive or parliamentary control (with the exception of high parliamentary surveillance[102]) and not removable by such authorities.

c. Standards applying to the approval of signals intelligence collection

Art. 5 IntelSA regulates the principles governing information gathering. For information gathering measures requiring authorisation and as explained above, please refer to Art. 26 ff. IntelSA and in particular Art. 27.

d. Use of information collected through non-individualized/programmatic signals intelligence limited to specified purposes

As explained under 4.2.1c.iv above, "non-individualized/programmatic collection" is subject to strict conditions. It is de facto restricted as the double authorisation procedure applies to the issuance of a such a mandate, which means that the proportionality and the necessity principles must be respected; moreover, it is also limited in time. Furthermore, if the service carrying out the communications intelligence 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 (see Art. 38 para. 6 IntelSA).

e. Documentation for signals intelligence activities

Art. 44 ff. IntelSA regulate data processing and archiving and art. 58 ff. IntelSA regulate storage of data from information gathering measures requiring authorisation.

According to the ordinance of 25 November 1998 on the Organisation of the Government and the Federal Administration (GAOO)[103] the FIS is obliged to provide evidence of its own business activities with the help of systematic business management (Art. 22 para. 1 GAOO in connection with Art. 52 IntelSA). The OA-IA bases its oversight on this documentation requirement.

Furthermore and according to art. 78 para. 4 and 5 IntelSA, the Independent Oversight Authority has access to all relevant information and documents and access to all the premises. It may request copies of documents and it may also have access to all the information systems and data collections.

---

[101] The Independent Oversight Authority for Intelligence Activities (OA-IA, see 4.2.5.a below) conducts an audit every year concerning the information gathering measures requiring authorisation. See the published annual reports: ab-nd.admin.ch/en/annual-report and the published audit-plans of the OA-IA and the published results of the audits on the website (the latter are not translated into English).

[102] High parliamentary surveillance does not involve instructions or the power to take decisions. It encompasses the power to control the financial management.

[103] https://www.fedlex.admin.ch/eli/cc/1999/170/fr (not available in English).

4.2.4 Post-collection handling of signals intelligence information

As a general remark, the approval measures along with the legal bases detailed above form a set of stringent conditions surrounding access to and processing of personal data. In addition, oversight and redress mechanisms are in place as described further below.

a. Standards applying to Swiss intelligence agencies' retention of information gathered and retention time periods

Art. 44 ff. IntelSA regulate data processing and archiving. In particular, Art. 45 notably states that the FIS shall assess the relevance and accuracy of personal data before recording it in an information system and that it shall only record data that may be used to fulfil its tasks as defined by the IntelSA. The FIS shall also periodically check in all information systems whether the recorded sets of personal data are still required to carry out its tasks and it shall delete data records that are no longer required.

The deletion of personal data from the FIS storage systems is regulated in Art. 8 ISSO-FIS. Art. 8 para. 2 ISSO-FIS provides a list of all articles in which the retention periods for each system are specified.

The maximum retention periods of data that do not require court authorisation vary in this case from 3 to 45 years, depending on the systems the data are kept in and the purpose for which they were collected. The retention periods of such data are regulated by the articles 7 para. 7, 21 para. 2, 28, 34 para. 2, 40, 45, 50, 55, 60, and 65 ISSO-FIS.

Provisions of the ISSO-FIS	Purposes of collection	Retention periods
Art. 7 para. 7	(general provision)	Data relating to operations is kept for a maximum of 45 years.
Art. 21	data on international terrorism	30 years maximum
	data on prohibited intelligence, dissemination of nuclear, biological or chemical weapons, including their means of delivery, and all goods and technologies for civilian or military purposes which are necessary for the manufacture of such weapons (NBC proliferation) or illegal trade in radioactive substances, war material and other weapons goods	45 years maximum
	data on entry bans	a maximum of 10 years after expiry of the entry ban, and a maximum of 35 years in all
	data relating to information relevant to security policy	45 years maximum

		Original documents that are not linked to a source document are kept for a maximum of 15 years
Art. 28	source documents in the IASA-EXTR SRC system	15 years maximum
Art. 34 para. 2	system for classifying, entering, processing, consulting and evaluating data from preliminary investigations by cantonal enforcement authorities (INDEX SRCant) and system for managing mandates and preparing, transmitting and filing reports from cantonal enforcement authorities, as well as for filing products received by the FIS	5 years maximum
Art. 40	filing and data processing system used to manage and control business processing, and to ensure the efficiency of work processes	20 years maximum
Art. 45	system comprising areas sorted by events and themes for classifying, processing, consulting and evaluating notably event-related data correlated with intelligence networks as well as periodic situation reports, situation monitoring and documentation.	3 years maximum
Art. 50	system for storing data classified by source and theme. It is used to search and evaluate data from public information sources	2 years maximum
Art. 55	Quattro P system (data obtained at border posts in the course of border and customs checks)	5 years maximum
Art. 60	data storage system for directing, controlling and reporting on radio and cable network exploration resources	5 years maximum after completion of the relevant exploration mandate

Art. 65	residual data storage system for storing data that has not been allocated directly to another information or storage system	5 years maximum

As regards personal data which are related to information gathering measures requiring authorisation, Art. 70 para. 1 ISSO-FIS regulates their retention periods. The FIS must erase data, which are not used in judicial proceedings or in an ongoing operation: (a) no later than 6 months after the notification of the measure to the data subject concerned under Art. 33 para. 1 IntelSA; (b) immediately after the entry into force of the decision on the exemption from the obligation to communicate the information to the data subject under Art. 33 para. 3 IntelSA[104]; (c) immediately after the entry into force of a decision on an appeal against the measure ordered. As regards data from foreign searches referred to in Art. 36 para. 5 IntelSA, the maximum retention period is three years (Art. 70 para. 3 ISSO-FIS).

With regard to data from information gathering measures requiring authorisation, the FIS shall store it on a case-related basis and separately from the information systems. 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 (Art. 58 IntelSA).

Finally, 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 protection period (Art. 68 Intel SA).

b. Requirements or constraints applying to sharing information gathered through signals intelligence with other intelligence agencies

Art. 11 IntelSA as well as the FISO regulate the cooperation and exchange of information between the FIS and the Swiss Armed Forces Intelligence Service (see. Art. 3 FISO). They shall cooperate closely in the areas of overlapping tasks (see Art. 6 IntelSA). They shall support each other in the performance of the tasks assigned to them, in particular by the regular transmission of information and assessments in areas where the tasks to be carried out overlap. Each service may request information from the other at any time.

Furthermore art. 4 FISO regulates the cooperation with the Military Security Service. The FIS supports the Military Security Service in protecting the armed forces against espionage, sabotage and other illegal acts.

The FIS shall ensure before disclosing any personal data or products that the personal data satisfies the legal requirements of the IntelSA and that its disclosure is lawful and necessary in the case concerned (see Art. 59 IntelSA). This means that the protection of sources and the third party rule must apply at all times.

c. Requirements or constraints applying to sharing information gathered through signals intelligence with law enforcement agencies

Art. 5 FISO regulates the cooperation between FIS and the Federal Office of Police (fedpol). They shall provide each other with all the information they require to fulfil their statutory duties.

---

[104] In this respect, it can be added that the guarantees of fundamental rights in the ECHR and the corresponding jurisprudence of the ECtHR have influenced and formed an essential basis for the IntelSA. This is demonstrated by the incorporating of Art. 33 para. 2 letter a IntelSA, which is inspired by the *Klass and Others v. Germany* ruling that subsequent notification could call into question the long-term purpose of surveillance, and that it is possible to waive it under certain conditions.

The FIS may provide fedpol with information if the FIS determines that this is required for fedpol to fulfill its statutory duties.

Art. 59 and 60 para. 2-4 IntelSA and Art. 32 and 34 FISO lay down the safeguards and limitations for the disclosure of personal data within the framework of the legally prescribed cooperation with law enforcement authorities. In particular, Art. 60 para 2 IntelSA states that where information obtained by the FIS may be used by other authorities (such as fedpol) 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. Art. 34 FISO specifies this article and indicates that disclosure of information to law enforcement authorities for use in a criminal proceeding shall be in the form of a written official report that is admissible in court.

A list of domestic authorities to whom the FIS shall disclose personal data if this is necessary in order to safeguard internal or external security (see Art. 60 para. 1 IntelSA) has been established according to Art. 32 para. 1 FISO in connection with Annex 3 FISO.

d. Requirements or constraints applying to sharing information gathered through signals intelligence with other Swiss government agencies or with foreign governments

Art. 19 and 20 IntelSA regulate the duties of the federal and cantonal authorities and organisations that the Confederation or the cantons have mandated to fulfil public tasks to provide information or to report. They are notably 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.

According to Art. 60(1) IntelSA, the FIS shall disclose personal data to domestic authorities if this is necessary in order to safeguard internal or external security[105]. Before disclosing any personal data, the FIS shall ensure that the data satisfies the legal requirements of the IntelSA and that the disclosure is lawful and necessary in the case concerned (Art. 59 IntelSA). The authorities to whom the FIS may disclose personal data in accordance with the mentioned legal requirements and the purposes for such disclosures are listed in Annex 3 of the FISO (see also Art. 32 para. 1 FISO).

Cooperation with foreign intelligence services and security services is regulated by art. 12 IntelSA as well as by art. 7 FISO, which notably stipulates that the FIS shall only maintain regular intelligence contacts with foreign agencies if it has been authorised to do so by the Federal Council.

Art. 59 and 61 IntelSA as well as Art. 35 FISO regulate the disclosure of personal data by the FIS to foreign authorities.

e. Non-relevance of nationality with respect to information gathered through signals intelligence

The nationality is not relevant for the authorisation procedure or the implementation of the surveillance measures. Furthermore, the principles of Art. 5 IntelSA (necessity and proportionality of the information gathering measure) as well as the provisions of Art. 59-62 IntelSA and Art. 32-35 FISO govern all types of information gathering.

f. Data security and access requirements applying to information gathered through signals intelligence

[105] The FIS has the discretion to make this determination.

According to Art. 7 IntelSA, the FIS shall take measures to guarantee the protection, safety and security of its employees, facilities and the data that it processes. Please also refer to 4.2.4.a above.

g. Constraints applying to government querying of information gathered through signals intelligence

The ISSO-FIS regulates the operation, content and use of information systems operated by the FIS. Section 3 ISSO-FIS contains general provisions on data protection and security, quality control, etc. Furthermore, the FIS processes particularly sensitive data outside its information systems if this is required for the protection of sources in accordance with Art. 35 IntelSA (Art. 7 ISSO-FIS).

According to Art. 5 para. 3 IntelSA, the FIS 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. Furthermore, the FIS may not gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland except 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.

Furthermore Art. 36 ff. IntelSA regulate the information gathering about events outside Switzerland.

Moreover, Art. 39 IntelSA on cable communications intelligence indicates that the search parameters must be defined so that their application causes as little interference as possible in the private domain of persons (see Art. 39 para. 3 IntelSA).

Finally and according to Art. 42 IntelSA, the FIS will not receive directly the data stored by the provider service but only those results which the provider service deems to correspond with the query[106]. All data protection rules, whether based on IntelSA or general Swiss data protection legislation, apply to those data passed on to the FIS.

h. Constraints applying to government non-individualized/programmatic querying of information gathered through signals intelligence

The IntelSA gives the FIS the power to conduct cable reconnaissance (surveillance) in order to gather information about security relevant incidents abroad (Art. 39 ff. IntelSA[107]). The cable surveillance covers specific border crossing communications (over international telecommunications cables) and is carried out by the Service for Actions in Cyberspace and Electromagnetic Space (ACEM) on behalf of the FIS. The ACEM filters the relevant data streams and forwards the results to the FIS.

As the aim of cable communications intelligence is not to identify and monitor specific persons or entities in Switzerland, but to gather information about events outside Switzerland that are of significance to security, searches are made using defined key words. In line with Art. 39 IntelSA, the ACEM may only transmit data from cable networks traffic to the FIS if they correspond to defined key words[108] 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. While an individualized suspicion is not explicitly required in this context, it is in practice more effective and less intrusive to search for specific personal details of a targeted

---

[106] Information about Swiss-Swiss communications will only be passed on under certain conditions (Art. 42 para. 2 IntelSA).

[107] See also Art. 25 ff. FISO, which regulate certain aspects of the intelligence measures mentioned in Art. 39 ff. IntelSA.

[108] Since the double authorisation procedure is applicable, it creates de facto restrictions on the selection of key words as the categories of key words must be authorised by the Federal Administrative Court.

person or for a telecommunications connection used by a targeted person than using a trivial search term. The FIS must submit the categories of the keywords to the Federal Administrative Court for approval[109]. The FIS must check the relevance and accuracy of data transmitted by the ACEM before putting them in its data bases (Art. 45 IntelSA).

In order to protect the fundamental rights of persons whose communications data are included in cable communications intelligence, but do not meet the search parameters of the FIS mandate, the ACEM as a third party triages the data from the forwarded cable networks traffic (Art. 42 para. 1 IntelSA). The ACEM only forwards data to the FIS that contain information within the search parameters clearly defined for the fulfilment of the mandate.

4.2.5 Oversight

a. Responsible oversight bodies

An independent supervisory authority, the Independent Oversight Authority for Intelligence Activities (OA-IA), was created on 1 September 2017 (Art. 76 ff. IntelSA). It supervises the intelligence activities of the FIS, the MIS and the ACEM. It publishes an annual activity report[110]. The OA-IA monitors and audits the legality of cable communication surveillance and the expediency and the effectiveness of FIS, MIS and ACEM activities with regard to radio and cable surveillance, including compliance of data collection with the principles set out in Art. 5 IntelSA, as well as compliance regarding maximum retention periods, and the handling by the intelligence services of requests of access to data by individuals.

There is also an independent control authority to oversee radio and cable surveillance (Art. 79 IntelSA): the Independent Control Authority for Radio and Cable Intelligence (ICA). The ICA is an independent body and not bound by directives from other authorities in carrying out its tasks (Art. 79 para. 1 IntelSA.) ICA members are appointed by the Federal Council for a four-year term of office and the Federal Council may remove ICA members only for cause[111]. As an internal administrative commission, it consists of three to five officials from the federal administration with expertise in the areas of fundamental rights protection, security policy and communications technology (Arts. 7(1)-(2) OSIA). The Federal Council is responsible for regulating its composition and the organization, the remuneration of its members, and the organization of its Secretariat (Arts. 8(3)-(4) OSIA. Decisions of the ICA require the approval of the majority of its members (Arts. 8(1)-(3) OSIA. It verifies the legality of radio communications intelligence and supervises the conduct of authorised and cleared cable communications intelligence assignments. In particular, the control authority examines the assignments given to the ACEM and the processing and passing of information, which the ACEM has obtained. Its organization[112] and tasks are governed by the OSIA.
The ICA ensures an additional and separate technical review of the radio and cable intelligence. In particular, it controls the legality and proportionality of orders of the FIS or the MIS to the ACEM for radio communications intelligence and monitors the implementation of orders

---

[109] The Federal Administrative Court will notably examine whether the information gathering measure is most suitable and necessary for achieving a specific information gathering objective and causes the least interference with the fundamental rights of the persons concerned. This implies that the Federal Administrative Court examines the proportionality of the information gathering measure as well as whether the categories of key words are necessary for the fulfillment of the order of the FIS in question.

[110] Annual Report of the OA-IA (admin.ch)

[111] Art. 76 para. 5 IntelSA applies by analogy, that is to say that removal would in principle need to be based on the same grounds as those listed for removal of the head of the OA-IA.

[112] As internal administrative commission, it consists of three to five officials from the Federal Administration with expertise in the areas of fundamental rights protection, security policy and communications technology, elected for a four-year term of office (Art. 79 para. 4 IntelSA, Art. 7 para. 1 and 2 OSIA). Although elected by the Federal Council and located within the Federal Administration (DDPS), both the IntelSA and OSIA contain a number of guarantees ensuring the independence of the ICA. Accordingly, its members are not bound by instructions when performing their task (Art. 79 para. 1 IntelSA). The DDPS neither chairs nor provides the majority of the members of this authority, but proposes them to the Federal Council for election (Art. 7 para. 3 and 4 OSIA). The supervisory authority organises itself, sets its own audit program and has its own secretariat, with resources provided by the DDPS. Decisions of the ICA require the approval of the majority of its members (Art. 8 para. 1-3 OSIA).

for cable intelligence, which are approved by the Federal Administrative Court (Art. 79 para. 1 IntelSA). The FIS and the MIS are obliged to notify the ICA of every new radio and cable intelligence order and to provide it with all the information necessary (Art. 9 para. 1 OSIA). The competent bodies shall give access to all relevant information and facilities to the ICA (Art. 79 para. 2 IntelSA). In the exercise of its control mandate, the ICA may in particular view relevant orders, applications and decisions with respect to cable intelligence, examine results of radio and cable intelligence on a random basis or examine the ACEM procedures, data and systems (Art. 10 para. 1 OSIA). As part of its audit activities, the ICA moreover carries out inspection visits to the competent bodies several times a year. In principle, radio and cable intelligence orders must be audited on an annual basis (Art. 10 para. 2 OSIA). Based on the review, the ICA presents recommendations[113] and applies to the DDPS for orders for radio intelligence to be ceased or information to the deleted (Art. 79 para. 3 IntelSA).
Both, the OA-IA and the ICA are authorised to initiate audits either acting on corresponding requests or pro-actively on their own volition (Art. 10 para. 1 lets. c-f OSIA).

In addition, there is a parliamentary oversight according to Art. 81 IntelSA. The Control Delegation (CDel) of the Federal Assembly (three members of the National Council and three members of the Council of States) monitors and controls the activities of the intelligence agencies. The CDel has unrestricted access to secret intelligence information. It issues recommendations and can carry out specific inspections. It has access at all times to the premises of intelligence services, its staff, databases and top-secret operational files. The CDel can request information from all institutions that perform federal tasks and question their representatives, including the members of the Federal Council. It can also ask the Federal Council to provide documents that supported the decision-making process in the Council itself. In fact, the foremost task of the Delegation is to make sure that the Federal Council abides by its own responsibilities for managing and controlling intelligence activities in accordance with the law.

The supervision of intelligence services by the OA-IA, the independent control authority and the CDel does not exclude the supervisory powers of the FDPIC which is entitled to and has legal obligation to monitor legal conformity of personal data processing by the federal bodies including intelligence services.

b. Independence of oversight bodies

The oversight bodies mentioned under 4.2.5.a. above are all independent.

Art. 77 stipulates that the OA-IA shall carry out its tasks independently; it is not bound by directives from other authorities. It has its own budget, appoints its own staff, constitutes itself and shall regulate its organisation and its working methods in its own procedural rules.

The head of the OA-IA is appointed by the Federal Council for a renewable period of six years. The Federal Council may remove him from the post only if he breaches his official duties willfully or through gross negligence, or if he becomes permanently incapable of exercising office (Art. 76 IntelSA).

[113] The ICA submits an annual report on its activities and the audit results to the head of the DDPS, who sends the report to the Federal Council and informs it about the recommendations of the ICA and their implementation (Art. 10 para. 3 OSIA). The results of the ICA's audit activities are confidential and are only submitted to the bodies provided by law, or bodies affected by the subject matter, i.e. the Federal Council, the Control Delegation of the Federal Assembly, the OA-IA and the Federal Administrative Court. Neither the reports of the ICA, nor its recommendations or proposals are public (Art. 79 para. 3 IntelSA).

According to Art. 79 IntelSA, the independent control authority 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. The independent control authority shall be granted access by the responsible agencies to all relevant information and facilities.

The independence of the FDPIC is prescribed by Art. 43 para. 3 FADP.[114]

c. Investigative authorities of oversight bodies

The OA-IA shall oversee the intelligence service activities carried out by the FIS and shall audit these activities to confirm their legality, expediency and effectiveness (Art. 78 para. 1 IntelSA). 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. (Art. 78 para. 4 IntelSA). In order to carry out its supervision activities, it may have access to all the information systems and data collections of the subjects of supervision; it may also have access to sensitive personal data. (Art. 78 para. 5 IntelSA).

The independent 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 (Art. 79 para. 2 IntelSA).

With regard to the FDPIC's investigative powers, see 2.2 above.

d. Access of oversight bodies to classified information

The oversight bodies have access to classified information necessary to perform their work and have the power to compel Swiss intelligence agencies to provide access to relevant classified information (see 4.2.5.c above and with regard to the FDPIC, see 4.2.5.b below).

e. Treatment of possible incidents of non-compliance

The dual approval process for information gathering measures requiring authorisation as well as the independent oversight system contribute to ensuring compliance. Art. 45 and 75 IntelSA regulate quality assurance. In particular, Art. 75 IntelSA requires self-control measures by the FIS; these would include reporting major incidents either to FIS' supervisory authorities, or the Federal Council, or both.

According to Art. 24 FADP, the agencies are required to report data protection breaches to the FDPIC.

f. Binding authority of oversight bodies to order intelligence agencies to adopt remedial measures when incidents of non-compliance are identified

The OA-IA shall provide the DDPS with a written report on the results of its audit. It may issue recommendations (Art. 78 para. 6 IntelSA).

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. 78 para. 7

[114] See also footnote 43 above.

IntelSA)[115]. Until today, all of the OA-IA's recommendations have been accepted. The OA-IA is informed about the implementation of the recommendations by the DDPS. If it is not satisfied with the information received, it can carry out an audit again (Art. 78 IntelSA).

According to Art. 79 para. 3 IntelSA, the independent control authority 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.

When the CDel has reason to believe that the intelligence services are not functioning according to the law, it can launch a proper investigation. Such an investigation results usually in a report that in most cases is fully published. Before publication of the findings of an investigation, the CDel habitually consults the authority or the service concerned in order to prevent the publication of information that would be harmful to national security.

The FDPIC's competences as regards incidents related to data protection are described above under 2.2.

4.2.6 Redress

Measures to collect personal data that infringe particularly strongly on the fundamental rights of data subjects (e.g. monitoring electronic communications or using tracking devices) are subject to a dual approval process as described above.

Rulings issued by federal bodies based on the IntelSA can be challenged before the Federal Administrative Court and, in second instance, before the Federal Supreme Court (Art. 83 para. 1 and 4 IntelSA). The term "ruling" is defined in Art. 5 of the Administrative Procedures Act[116] and refers to decisions by which a competent authority authoritatively determines rights and obligations of an individual person in a specific individual case. According to article 44 APA, only rulings constitute admissible objects of appeal.[117] An unlawful processing of personal data by the FIS, on the other hand, would have to be qualified as a real act. In order to challenge the unlawfulness of such processing, the data subject has the right to request from the FIS to issue a respective ruling[118], which can be challenged before the Federal Administrative Court based on Art. 83 para. 1 IntelSA.

This means that a person may challenge a decision or ruling of a federal body, notably the FIS, before the Federal Courts (first before the Federal Administrative Court and in a second instance before the Federal Supreme Court), may it be for unlawfully processing data collected through intelligence measures or for conducting unlawful surveillance. In such cases the Federal Courts have access to all relevant documents[119] and can provide redress. For an example of decision, please refer to 4.2.1.c.iv. above.

---

[115] The recommendations must be implemented and any related decision of the Federal Council is binding on the FIS.

[116] Federal Act of 20 December 1968 on Administrative Procedure (APA), SR 172.021). Art. 5 APA states that rulings are decisions of the authorities in individual cases that are based on the public law of the Swiss Confederation and have as their subject matter a. the establishment, amendment or withdrawal of rights or obligations, b. a finding of the existence, non-existence or extent of rights or obligations, c. the rejection of applications for the establishment, amendment, withdrawal or finding of rights or obligations, or the dismissal of such applications without entering into substance of the case. Rulings are moreover enforcement measures, interim orders, decisions on objections, appeal decisions, decisions in a review and on explanatory statements.

[117] As most important form of government action, rulings conclude the internal administrative procedure and are objects of appeal of the external, contentious appeal procedure.

[118] Based on the constitutionally guaranteed fundamental right to judicial protection (article 29*a* Swiss Federal Constitution), article 25*a* APA provides legal protection for administrative acts that are not subject to appeal like rulings. Accordingly, any person who has a (legal or factual) interest worthy of protection may request from the authority that is responsible for an act based on federal public law and which affects rights or obligations, that it a. refrains from, discontinues or revokes unlawful acts, b. rectifies the consequences of unlawful acts, or c. confirms the illegality of such acts. The authority shall decide by way of a ruling (article 25*a*(2) APA).

[119] A special procedure has been set up with the Federal Administrative Court for the management of secret-classified information.

After exhausting possibilities of redress at national level, cases may be brought to the ECtHR.

a. Constraints applying to an individual person (including a U.S. person) having his or her claim of unlawful signals intelligence heard in the general courts of Switzerland, if the claimant does not know whether his/her data has in fact been accessed by Swiss intelligence agencies

According to Art. 33 IntelSA, 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.

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; or d. the person concerned cannot be contacted.

If one of these conditions applies in an individual case, a balancing of interests is carried out by the FIS in order to decide on a postponement. The postponement decision needs an authorisation of the Federal Administrative Court and clearance of the DDPS (Art. 33 para. 3 and 29 IntelSA). The postponement (and the dispense) does not affect the right of access to data.

In any case and as is mentioned above (4.2.1 answer to question c.iv.), the Federal Supreme Court has with its judgment 1C_377/2019 implemented the constant jurisprudence of the ECtHR by confirming the right of everyone to challenge interceptions over cables and to file an individual complaint against secret mass surveillance systems as a whole to be reviewed by at least one national independent authority.

b. Non-judicial redress mechanism for complaints alleging violations of Swiss law by Swiss intelligence agencies

According to Art. 25 FADP anyone with a legitimate interest may request the federal body concerned (thus also the FIS) to (a) refrain from processing personal data unlawfully; (b) eliminate the consequences of unlawful processing; (c) ascertain whether processing is unlawful. The applicant may in particular request that the federal body corrects or destroys the personal data or blocks its disclosure to third parties.

Data subjects have the right of access to data concerning them that are processed in the FIS's information systems. The right of access is governed by the FADP for certain information systems of the FIS (Art. 63 para. 1 IntelSA) and by the IntelSA for the remaining information systems (Art. 63 para. 2 IntelSA). The right to access is deferred if there are (a) overriding public interests connected with the fulfilment of a task in accordance with Art. 6 IntelSA, or a prosecution or other investigation, (b) overriding interests of third parties, or (c) if no data about the applicant has been processed.

If the access is deferred, the FIS must inform the applicant that he or she has the right to request the FDPIC to examine whether the data, if any, was lawfully acquired or is being lawfully processed[120] and whether overriding interests in preserving secrecy justify the deferral (Art. 63 para. 3 IntelSA). The FDPIC conducts an examination if so requested by the applicant (Art. 64

[120] See Art. 5 letter d FADP: *processing* means any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data.

para. 1 IntelSA). In this respect the right to information is governed by the FADP according to Art. 63 IntelSA. The FADP does not require the request for information to be substantiated so that it can be claimed unconditionally (Art. 25 para. 1 FADP). The examination of the FDPIC covers all of the forms of signals intelligence. The FDPIC must hear all claims (including by foreign nationals). The FDPIC is independent (see footnote and comment under 2.2. on page 7). The FDPIC has full access to classified information necessary to their examination[121]. The FDPIC may issue a decision to the FIS (which can be appealed to the Federal Courts), which confers the FDPIC binding authority over Swiss intelligence agencies to require appropriate remediation. According to Art. 64 para. 2 IntelSA, the applicant is notified either that no data has been unlawfully processed or that the FDPIC has identified errors relating to the processing of data or the deferral of the provision of information and that they have opened an investigation in accordance with Art. 49 FADP.

[121] The full access of the FDPIC to the classified information necessary for the handling of a complaint results from various legal provisions of the IntelSA as well as the FADP. Firstly, it should be noted that Art. 4 FADP, which regulates the personal scope of application of the FADP, does not exclude the intelligence service from the supervisory competence of the FDPIC. Furthermore, Art. 49 FADP provides that the FDPIC shall open an investigation onto a federal body ex officio or in response to a report if there are sufficient indications that a data processing activity could violate data protection regulations. The federal body is then obliged to provide the FDPIC with all the information and documents necessary for the investigation. Should the federal body fail to fulfil its obligation, the FDPIC may order various measures according to Art. 50 FADP (e.g. access to all information, documents, records of processing activities and personal data that are required for the investigation; access to premises and installations; questioning of witnesses; appraisals by experts). The IntelSA does not impose any restrictions on the FDPIC's access to classified information. This is indirectly confirmed by Art. 63 para. 3 IntelSA, which authorises the FDPIC to consult any existing data and to balance the interests of secrecy and the disclosure of such data.