Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP

Federal Office of Justice FOJ
Public Law Division
Legislative Projects I

30 April 2024

Assessment of adequacy – United States

Establishment of a framework for transferring personal data from Switzerland to certified organisations in the United States *(Swiss–U.S. Data Privacy Framework*) – Assessing the adequacy of the level of protection of personal data

BJ-D-E3D83401/174

Bericht

Table of Contents

1 Background 4

1.1 Adequacy regime introduced by the Data Protection Act of 25 September 2020 .. 4

1.2 Previous framework and invalidation 4

1.3 Establishment of a framework for the transfer of personal data from Switzerland to certified organisations in the United States 5

2 Adequacy assessment criteria 5

Bericht

1 Background

1.1 Adequacy regime introduced by the Data Protection Act of 25 September 2020

The new data protection legislation, which has been in force since 1 September 2023, has introduced a change in responsibilities. Under Article 16 paragraph 1 of the Data Protection Act of 25 September 2020 (FADP)[1] and Article 8 paragraph 1 of the Data Protection Ordinance of 31 August 2022 (DPO)[2], the Federal Council is responsible for determining whether a state, a territory, a specified sector in a state or an international body guarantees an adequate level of data protection. Annex 1 DPO lists the states, territories, specific sectors in a state and international bodies that guarantee an adequate level of data protection.

In addition, the Federal Office of Justice is responsible for assessing the adequacy of the level of data protection[3]; this assessment is legal in its nature and is published.

1.2 Previous framework and invalidation

Under the Data Protection Act of 19 June 1992 (now repealed), the Federal Data Protection and Information Commissioner (FDPIC) maintained a list of countries that offered an adequate level of data protection.

On 11 January 2017, the FDPIC added the United States to its list of states for data exchanges with companies certified under the Swiss-U.S. Privacy Shield. The EU had a virtually identical framework with the United States.

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling in the so-called Schrems II case (Case C-311/18) which found that the protection afforded was insufficient, thereby invalidating the mechanism for transferring personal data from the EU to the U.S. on the grounds that it allowed disproportionate derogations from data protection with regard to surveillance by the U.S. intelligence services and offered no effective means of redress to the data subjects.

Even though the CJEU's decision is not binding on Switzerland, in view of the general principle of the rule of law and the need for legal certainty, and considering that the framework governing the exchange of personal data between Switzerland and the United States was virtually identical to that existing between the EU and the United States, the FDPIC considered that it was appropriate to re-examine the presence of the United States on its indicative list of states that guarantee an adequate level of protection. On 8 September 2020, the FDPIC published a position paper in which expressed the opinion that the United States did not meet the requirements of adequate data protection in terms of the Data Protection Act and removed the United States from its list. As a result, the Federal Council did not include the United States in the list of states in Annex 1 DPO when the new legislation came into force on 1 September 2023.

---

1 SR 235.1.

2 SR 235.11.

3 In accordance with Article 7 paragraph 1 letter d of the Organisation Ordinance for the Federal Department of Justice and Police (SR 172.213.1), this task is performed in collaboration with other competent offices.

1.3 Establishment of a framework for the transfer of personal data from Switzerland to certified organisations in the United States

After the previous framework between the United States and Switzerland had been removed from the FDPIC list, discussions took place between the United States and Switzerland, in parallel with the discussions between the United States and the European Union.

These discussions led to the establishment of a commercial framework for certified organisations (principles, including supplemental principles, of the data protection framework between Switzerland and the United States), the publication of various documents by the U.S. government and by the relevant authorities in the United States (Executive Order 14086 of 7 October 2022, Regulation on the Data Protection Review Court issued by the U.S. Attorney General on 7 October 2022, Intelligence Community Directive 126 issued by the Office of the Director of National Intelligence (ODNI) on 6 December 2022), the designation of Switzerland on 7 June 2024 as a state benefiting from the two-tier redress mechanism including access to the Data Protection Review Court, and the delivery of letters from the competent authorities in the United States confirming the commitments made. Taken together, these documents, which can be accessed via the links to the reference texts included at the end of this document, constitute the *Swiss–U.S. Data Privacy Framework (Swiss–U.S. DPF*) for the transfer of personal data from Switzerland to certified organisations in the United States.

The purpose of the review below is to assess whether all of these documents enable the United States to guarantee an adequate level of protection of personal data when data is transferred between controllers or processors in Switzerland and certified organisations in the United States pursuant to the assessment criteria set out in the DPO.

2 Adequacy assessment criteria

Article 8 DPO sets out a number of criteria that must be taken into account when assessing adequacy:

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, in particular of 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.

Annex 1 DPO lists the states, territories, specified sectors in a state and international bodies that guarantee an adequate level of data protection. This list is binding.

An adequate level of protection means a level of protection that is essentially equivalent to that provided by Swiss data protection law. The intention is not to compare the systems in place point by point, but to determine whether, as a whole, the system provided for by a state, a territory, a specified sector in a state or an international body ensures an essentially equivalent level of protection in terms of the content of the privacy rights guaranteed, the implementation of these rights and the means of control employed. In this context, account must be taken of the differences in legal and cultural traditions between a state, a territory, a specific

sector in a state or an international body that is the subject of an adequacy assessment and Switzerland.

The EU uses very similar criteria when assessing the adequacy of the level of protection of personal data from third countries in accordance with Article 45 of the General Data Protection Regulation[4].

3 Commercial framework for transfers of personal data between data controllers or processors in Switzerland and certified organisations in the United States

3.1 Applicable legislation

3.1.1 Main principles

The principles, including the supplemental principles, of the framework for the transfer of personal data from Switzerland to certified organisations in the United States (referred to below as the Swiss-U.S. DPF principles or the Principles)[5] are based on a certification system whereby organisations, i.e. businesses, in the United States that wish to benefit from the framework for the transfer of personal data undertake to comply with a set of privacy protection principles. In order to be certified under the Swiss-U.S. DPF, an organisation must be subject to the investigative and enforcement powers of the Federal Trade Commission or the Department of Transportation; in addition, it must certify that it adheres to the principles on an annual basis.

The Swiss-U.S. DPF principles define personal data as data about an identified or identifiable person that are within the scope of the FADP and its ordinances, received by an organisation in the United States from Switzerland, and recorded in any form. Furthermore, the Principles define processing as any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction. These important concepts are therefore defined in the same way as in Swiss law.

The Swiss-U.S. DPF principles guarantee compliance with the essential principles applicable under Swiss data protection law, as defined in particular by Article 6 of the FADP.

Personal data must therefore be processed lawfully and proportionally, be collected for a specific purpose and further used in a manner compatible with that purpose. In the Swiss-U.S. DPF, this results primarily in the Data Integrity and Purpose Limitation principle, and also the Choice principle, since an organisation must offer data subjects the choice of determining whether their personal data may be disclosed to a third party or used for a purpose that is materially different from that for which it was initially collected or subsequently authorised by them.

Personal data must be accurate and processed in a way that is proportionate to the purpose for which they are processed, and must not be kept for longer than is necessary for the purpose for which they were collected. In the Swiss-U.S. DPF, these notions are found in the Data Integrity and Purpose Limitation principle and the Choice principle.

---

[4] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 of 4.5.2016, p. 1, accessible under the following link: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu).

[5] See links to reference texts at the end of the document.

Bericht

Data security must be guaranteed: data controllers and processors must take reasonable security measures appropriate to the risks presented by the processing and the nature of the data processed. In the Swiss-U.S. DPF, this is found in the Security principle.

In accordance with the principle of transparency, data subjects must be informed of the main features of the processing of their personal data: in particular, organisations must inform data subjects of their participation in the Swiss-U.S. DPF, the type of data collected, the purpose of the processing, their rights and the legal redress available to them. In the Swiss-U.S. DPF, this is found in the Notice principle. Organisations are required to inform the public of their privacy policies reflecting the principles of the Swiss-U.S. DPF.

Data subjects have certain rights which may be enforced against the controller or processor, in particular the right of access to data, the right to object to processing and the right to have data rectified and deleted. Thus, data subjects have the right, without the need for justification, to obtain confirmation of whether personal data related to them is being processed, to have the data communicated to them and to obtain information about the purpose of the processing, the categories of personal data being processed and the recipients to whom the data is disclosed. The right of access may only be restricted in exceptional circumstances similar to the ones provided under Swiss law, in particular where the legitimate rights of others would be violated. In addition, data subjects have the right to obtain rectification or amendment of inaccurate data, and to obtain deletion of data that has been processed in violation of the Principles. Under the Swiss-U.S. DPF, this is covered by the Access principle and the supplemental principle on Access.

Specific rules apply to onward transfers of personal data between a certified organisation and a third-party controller or processor in accordance with the Accountability for Onward Transfer principle. An onward transfer can only take place for limited and specified purposes, on the basis of a contract and only if that contract requires the third party to provide the same level of protection as the one guaranteed by the Principles.

Under the Recourse, Enforcement and Liability principle, certified organisations must put in place effective mechanisms to ensure compliance with the Principles. Organisations must also take measures to verify that their privacy policies conform to the Principles and are in fact complied with. This can be done either by a system of self-assessment or by external compliance checks.

In addition, specific safeguards apply to the use of sensitive data as defined in Swiss law: organisations must obtain the express consent of the data subjects to disclose such data to a third party or use such data for purposes other than those for which they were collected or subsequently authorised by those individuals as part of the exercise of their choice (opt-in). However, it is not necessary to obtain this consent in certain limited circumstances, similar to the exceptions provided for in Swiss law, for example when the overriding interests of a third party so require. Under the Swiss-U.S. DPF, this is covered by the principle of Choice and the supplemental principle on Sensitive Data.

3.1.2 Scope

The commercial framework applies to personal data[6] transferred from Switzerland to organisations in the United States that have certified their adherence to the Principles (see 3.1.1. above).

This applies to organisations in the United States qualified as data controllers within the meaning of Article 5 letter j FADP or data processors within the meaning of Article 5 letter k FADP. Processors must be contractually bound to act only on the instructions of the controller in Switzerland and to assist the controller in responding to individuals exercising their rights under the Principles.

3.2 Safeguards in place, independent authority, legal remedies

3.2.1 Management of the commercial framework, certification and monitoring

The commercial framework is managed by the U.S. Department of Commerce (DoC).

To initially self-certify or subsequently re-certify (on an annual basis) under the Swiss-U.S. DPF, organisations are required to publicly declare their commitment to respect the Principles and to make their privacy protection policies available and fully implement them. Organisations must also provide the DoC with information most particularly concerning the purposes for which personal data will be processed, the relevant independent recourse mechanism and the statutory body responsible for ensuring compliance with the principles. Organisations self-certifying for the first time are not permitted to refer publicly to their adherence to the Principles until the DoC has added the organisation to the list of participating organisations that is maintained and made available to the public by the DoC.

The DoC is also responsible for oversight. To ensure the correct application of the Swiss-U.S. DPF, the DoC will maintain and make available to the public a list of organisations that have self-certified to the DoC and declared their commitment to adhere to the Principles so that they can be identified as such, as well as a register of organisations that have been removed from the list, specifying in each case the reason for the removal. The DoC will remove from the list those organisations that voluntarily withdraw from the Swiss-U.S. DPF or fail to complete their annual re-certification to the DoC; these organisations must either continue to apply the Principles to the personal data they received under the Swiss-U.S. DPF and affirm to the DoC on an annual basis their commitment to do so (i.e., for as long as they retain such data), provide adequate protection for the personal data by another authorised means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses approved, established or recognised by the FDPIC), or return or delete the data. The DoC will also remove from the list those organisations that have persistently failed to comply with the Principles; these organisations must return or delete the personal data they received under the Swiss-U.S. DPF.

The DoC is responsible for carrying out checks to ensure that the certification requirements have been met, and in particular that the Principles have been complied with. In particular, it will carry out ‘spot checks’ on randomly selected organisations, as well as ad hoc spot checks on specific organisations when potential compliance issues are identified, particularly if the DoC receives complaints or if the organisation fails to respond satisfactorily to requests for

[6] Exceptions are data collected for publication, broadcast or other forms of public communication of journalistic material and information contained in material already published and broadcast from media archives.

information. In some cases, the organisation may be referred to the relevant authority for possible enforcement action.

The DoC will carry out checks to ensure that there have been no false claims of adherence to the Principles, particularly in the case of organisations that are removed from the list. If necessary, it may refer the matter to the competent authority for possible enforcement action.

3.2.2 Guaranteed application of the framework

In order to participate in the commercial framework, organisations must be subject to the jurisdiction of the relevant authorities in the United States, i.e. the Federal Trade Commission (FTC) or the Department of Transportation (DoT). These authorities have the investigatory and enforcement powers required to effectively ensure compliance with the Principles[7].

The FTC is an authority comprising five commissioners appointed by the President of the United States; their appointment must then be confirmed by the Senate. The commissioners are not permitted to engage in any other activity or employment during their seven-year term of office and may only be dismissed by the President for just cause. The FTC's mission is to protect the public from deceptive or unfair commercial practices and unfair methods of competition. It may investigate compliance with the Principles, as well as false claims of adherence to the commercial framework. The FTC can request administrative or federal court orders; it can monitor compliance with these orders by compelling organisations to produce documents and can use the judicial system to enforce these orders in the event of non-compliance.

The DoT has exclusive jurisdiction to regulate the privacy practices of airlines; in the case of travel agency practices relating to air transportation or the sale of air transportation services, this jurisdiction is shared with the FTC. If a settlement cannot be reached, the DoT may ask an independent and impartial DoT administrative judge to issue cease and desist orders or impose civil penalties, or may seek the same relief in the U.S. courts[8]. The DoT has also undertaken to give priority to investigations into alleged breaches of the Principles, to take appropriate enforcement action in cases of false claims of adherence to the commercial framework and to monitor and publish enforcement orders relating to the framework.

In view of the above, the FTC and the DoT can be described as independent supervisory authorities with sufficient powers and competences to ensure an adequate level of protection for personal data.

3.2.3 Legal remedies

As part of their certification, organisations must satisfy the requirements of the principle of Recourse, Enforcement and Liability by providing for effective and readily available independent recourse mechanisms (see Section 3.1.1.) by which disputes can be investigated and expeditiously resolved at no cost to the data subject.

Organisations may choose independent recourse mechanisms in Switzerland or the United States, and may opt for privacy protection programmes developed by the private sector that incorporate the principles into their regulations, statutory or regulatory oversight authorities

[7] See letters from the FTC and the DoT, accessible via the links to the reference texts at the end of the document.

[8] See Title 49 of the United States Code, regulations relating to transportation, available at the following link : 49 USC Ch. 461: INVESTIGATIONS AND PROCEEDINGS (house.gov).

that provide for the handling of individual complaints and the resolution of disputes, or a commitment to cooperate with the FDPIC.

Data subjects can file a complaint directly with an organisation, with an independent dispute resolution body designated by the organisation, or with the FDPIC. The DoC will refer organisations that fail to resolve a dispute to the FTC and DoT. The FTC and the DoT will give priority consideration to referrals of non-compliance with the Principles from the DoC and FDPIC. Data subjects can also file complaints directly with the FTC through the Consumer Sentinel database and may use the DoT's website to directly file privacy complaints against airlines and ticket agents.

Both the organisations and the responsible independent recourse mechanisms are required to respond promptly to complaints. If an organisation fails to comply with the decision of an independent dispute resolution body or government agency, this may result in removal from the list maintained and made available to the public by the DoC.

Data subjects may also file a complaint with the FDPIC. In addition, in order to expedite the processing of individual complaints, a DoC contact point liaises directly with the FDPIC. This enables data subjects to file complaints directly with the FDPIC and to have them forwarded to the DoC as the authority responsible for administering the commercial framework; this may result in removal from the list maintained and made available to the public by the DoC.

If a data subject's complaint has not been resolved by one of the above mechanisms, the data subject may under certain conditions invoke the binding arbitration option as described in Annex I of the Principles. Under this option, which can only be used as a last resort, an arbitration panel made up of one or three arbitrators (depending on the wishes of the parties) has the authority to order individual-specific, non-monetary relief (such as access, correction, deletion, or return of the data in question). A list of arbitrators will be drawn up jointly by the DoC and Switzerland on the basis of their independence, integrity and experience. The International Centre for Dispute Resolution (ICDR) of the American Arbitration Association[9] will administer the disputes. Proceedings before an arbitration panel are governed by a set of agreed arbitration rules and a code of conduct for arbitrators. Arbitration awards can be enforced in the U.S. courts[10].

The guarantee of legal redress is thus ensured when the legal remedies described above make it possible to ensure that complaints relating to non-compliance with the Swiss-U.S. DPF principles by certified organisations will be the subject of decisions and effective recourse mechanisms.

4 Access to personal data transferred by public authorities from Switzerland to the United States

4.1 Access for criminal law enforcement purposes

4.1.1 Applicable law, safeguards in place

The U.S. Constitution guarantees that the U.S. government does not have limitless, or arbitrary, powers to seize personal data. The purpose of the Fourth Amendment[11] is to protect the

[9] The Centre's website will provide clear and concise information on the arbitration mechanism and the procedure for requesting arbitration when the commercial framework comes into force: https://go.adr.org/sw-us_dpf_annexi.html.

[10] See Title 9 of the United States Code (US Code), regulations relating to arbitration, available at the following link: ARBITRATION (house.gov).

[11] See text of the U.S. Constitution, available at the following link: U.S. Senate: Constitution of the United States.

privacy and security of individuals against arbitrary invasions by government agents. The standards relating to the issue of a warrant apply both to physical searches and seizures and to seizures of electronically stored content. Even when a warrant is not needed, the Fourth Amendment requires that government activity be reasonable.

Personal data processed by certified organisations may be consulted for criminal law enforcement purposes by federal prosecutors[12] and federal investigative agents in accordance with the procedures described below. [13]It should be noted that these procedures apply regardless of the nationality or place of residence of the data subjects.

A subpoena may be issued by a grand jury in the context of investigations of certain serious crimes, usually at the request of a federal prosecutor, to require someone to produce or make available business records, electronically stored information, or other tangible items[14]. In addition, the use of administrative subpoenas may be authorised to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations. In both cases, the information must be relevant to the investigation and the subpoena must be reasonable, i.e. it must not be overbroad, oppressive or burdensome, otherwise it may be challenged by its recipient on those grounds.

In addition, legal provisions[15] allow the authorities responsible for enforcing criminal law to obtain access to communications data. A court may issue an order authorising the collection of real-time, non-content dialling, routing, addressing and signalling information about a phone number or e-mail if it is certified that the information likely to be obtained is relevant to an ongoing criminal investigation. The use of trap and trace devices may be authorised for a maximum period of sixty days, which may only be extended by a new court order. In addition, access to subscriber information, traffic data and stored content of communications held by internet service providers, telephone companies, and other third-party service providers may be obtained on the basis of a warrant from a judge based on probable cause to believe that the account in question contains evidence of a crime. For subscriber registration information, IP addresses and billing information, criminal law enforcement authorities may use a subpoena. For most other stored, non-content information, a criminal law enforcement authority must obtain a court order, which will be issued if the judge is satisfied that there are reasonable grounds to believe that the requested information is relevant and material to an ongoing criminal investigation.

Criminal law enforcement authorities may also intercept in real time wire, oral or electronic communications on the basis of a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a crime, or the whereabouts of a fugitive fleeing from prosecution.

If there is a presumption that seizable items are likely to be found, for example as evidence of an offence, a judge may issue a search or seizure warrant. However, a data subject may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial. Moreover, when a data holder, such as

---

[12] Federal prosecutors are agents of the Department of Justice.

[13] Federal investigative agents are affiliated with the Federal Bureau of Investigation (FBI), which is part of the Department of Justice.

[14] See Federal Rules of Criminal Procedure, available at the following link: Current Rules of Practice & Procedure | United States Courts (uscourts.gov).

[15] See Title 18 of the United States Code, regulations relating to offences and criminal procedure (in particular Sections 2510ss, 2701ss and 3121ss), accessible under the following link: OLRC Home (house.gov).

a certified company, is required to disclose data pursuant to a warrant, it may challenge the requirement to disclose as unduly burdensome[16].

In addition to the framework set by the above-mentioned legal provisions for access to data by federal public authorities for criminal law enforcement purposes, the U.S. Attorney General has published guidelines which impose additional limits on access and which also contain privacy protection clauses. This is particularly true of the Attorney General's Guidelines for domestic operations conducted by the Federal Bureau of Investigation[17], which require the FBI to use the least intrusive investigative methods possible and to take account of the invasion of privacy and potential damage to reputation.

Similar guarantees apply to investigations carried out under state legislation. The authorities responsible for enforcing the criminal law in the U.S. states use warrants and subpoenas in essentially the same way as described for the federal authorities, but sometimes with additional safeguards provided by the constitutions or legislations of the states. In any event, the guarantees provided at state level must be at least equal to those in the U.S. Constitution.

Similar safeguards apply to administrative subpoenas issued to obtain access to data held by companies in the United States for civil or regulatory purposes, i.e. that the procedure must be in the public interest. Authorities with civil and regulatory responsibilities may only request access to data that are relevant to matters within their regulatory powers[18]. In addition, the recipient of an administrative subpoena may challenge its enforcement in court, as the subpoena must be reasonable[19]. Although the use of an administrative subpoena is not subject to prior judicial approval, it becomes subject to judicial review if it is contested by the recipient or if the authority that issued the subpoena wishes to enforce it in court. In addition to these general guarantees, more stringent specific requirements may be derived from certain laws[20]. In any event, the requirements of the Fourth Amendment to the U.S. Constitution must be met.

It should be noted that the United States, through the Department of Justice, has also provided a letter confirming the applicable guarantees and limits on access described above[21].

The subsequent use of the data collected is governed by a central policy (Office of Management and Budget (OMB) Circular No. A-130[22]) which must be implemented and complied with by all federal authorities, including law enforcement authorities, when processing identifiable personal data. The authorities are required to 'limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of authorised agency functions'. Authorities must put in place a comprehensive privacy protection programme (e.g. managing risks, detecting, documenting and reporting incidents, etc.).

---

16 See Federal Rules of Criminal Procedure.

17 These guidelines can be accessed at the following link: The Attorney General's Guidelines for Domestic FBI Operations (justice.gov).

18 With regard to this, the case law of the Supreme Court has also clarified the need to balance the importance of the public interest in the information being requested with the importance of personal and organisational privacy interests. See *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), available at the following link: U.S. Reports: Okla. Press Pub. Co. v. Walling, 327 U.S. 186 (1946). (loc.gov).

19 See criteria mentioned above in relation to subpoenas as part of criminal investigations.

20 For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations, see in particular Title 31 of the United States Code, regulations relating to money and finances, available at the following link: OLRC Home (house.gov).

21 See letter from the DoJ, accessible using the links to reference texts at the end of the document.

22 Accessible at the following link: Review-Doc-2016--466-1.docx (archives.gov).

In addition, the E-Government Act[23] requires all federal agencies to put in place data security protection measures that are commensurate with the risk and magnitude of the harm that would result from unauthorised access, use, disclosure, disruption, modification, or destruction of data. They must also appoint a Chief Information Officer to ensure compliance with data security requirements and carry out an independent evaluation each year. Data protection impact assessments are required for all federal authorities that develop or acquire new information technologies which collect, store or disseminate data in an identifiable form or that introduce a new collection of data.

The OMB and the National Institute of Standards and Technology (NIST) have developed standards which are binding on federal agencies (including criminal law enforcement authorities) and that further specify the minimum data security requirements that have to be put in place, including access controls, ensuring awareness and training, contingency planning, incident response, auditing and accountability tools, ensuring system and information integrity, conducting privacy and security risk assessments, etc.[24]

The regulations on federal documents[25] stipulate that data held by the federal authorities must be subject to protection measures guaranteeing the physical integrity of the data and preventing unauthorised access.

As regards data retention, U.S. federal agencies are required to establish retention periods, which must be approved by the National Archives and Record Administration[26]. The length of the retention period is fixed in light of different factors, such as the type of investigation, or the relevance of the evidence to the investigation.

4.1.2 Independent authority, redress

4.1.2.1 Oversight

The activities of federal criminal law enforcement agencies are subject to oversight by various bodies[27]. As indicated in Section 4.1.1, in many cases this involves a prior review by the judiciary, which must authorise the various data collection measures. In addition, other bodies oversee the activities of criminal law enforcement authorities. These judicial and non-judicial bodies guarantee independent oversight.

Firstly, Civil Liberties and Privacy Officers (CLPO) are in place within various departments with criminal law enforcement responsibilities[28]. Their powers typically encompass the supervision of procedures to ensure that the respective authority is appropriately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated. The heads of each authority must ensure that the officers have the documents and resources required, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes. Officers must

[23] See Title 44 Chapter 36 of the United States Code.

[24] See OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Control Mappings to ISO/IEC 27001, July 2023, available at the following link: SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov).

[25] See Title 44 Chapter 31 of the United States Code.

[26] See Title 44 Chapter 29 of the United States Code.

[27] The mechanisms mentioned in Section 4.1.2.1. also apply to the collection and use of data by the federal authorities for civil and regulatory purposes. The federal civil and regulatory authorities are subject to the oversight of their respective Inspectors General and of Congress.

[28] See Title 42 Chapter 21E of the United States Code.

report regularly to Congress, in particular on the number of complaints received by the authorities concerned, their nature and the action taken, as well as the impact of their activities as delegates.

In addition, an independent[29] Inspector General[30] oversees the activities of the DoJ, including those of the Federal Bureau of Investigation. The Inspector General is responsible for independently investigating, auditing and inspecting DoJ programmes and activities[31]. He or she has access to all relevant files, reports, audits, reviews, documents, recommendations or other items, if necessary by subpoena, and may take testimony from witnesses. If the Inspector General makes non-binding recommendations for corrective action, his or her reports are generally made public and forwarded to Congress, which can then exercise its oversight function. The Inspector General accepts and investigates complaints from individuals.

In addition, to the extent they carry out counter-terrorism activities, authorities with criminal law enforcement responsibilities are subject to oversight by the Privacy and Civil Liberties Oversight Board (PCLOB). The Oversight Board is an independent agency within the executive branch composed of five members appointed by the U.S. President for a fixed six-year term with Senate approval; it may not have more than three members from the same political party[32]. The Oversight Board has responsibilities in the field of counter-terrorism policies and their implementation, with a view to protecting privacy and civil liberties. It may access all relevant files, reports, audits, reviews, documents and recommendations of the federal authorities, including classified information, and may take testimony from witnesses. It receives reports from the civil liberties and privacy officers of several federal authorities, may issue recommendations to the government and law enforcement authorities, and regularly reports to congressional committees and the President. The reports must be made publicly available to the greatest extent possible.

Finally, criminal law enforcement activities are subject to oversight by specific committees in the U.S. Congress (the House and Senate Judiciary Committees). The Judiciary Committees conduct regular oversight in different ways, in particular through hearings, investigations, reviews and reports.

4.1.2.2 Redress

Criminal law enforcement authorities must in most cases obtain prior judicial authorisation to collect personal data. Although this is not required for administrative subpoenas, these are limited to specific situations and will be subject to independent judicial review, at least where the government seeks enforcement in court. In particular, recipients of administrative subpoenas may challenge them in court on the grounds that they are unreasonable, i.e. overbroad, oppressive or burdensome. Data subjects may lodge requests or complaints with criminal law enforcement authorities concerning the handling of their personal data. In particular, they can request access to and correction of their personal data[33]. As regards activities relating to

[29] See Title 5 Part I Chapter 4 of the United States Code.

[30] Inspectors General have secure tenure and may only be removed by the President who must communicate to Congress in writing the reasons for any such removal.

[31] See DoJ Inspector General's 2020-2024 Strategic Plan, available at the following link: Strategic Plan Draft - To AIGs (justice.gov).

[32] See Title 42 Chapter 21E of the United States Code.

[33] See OMB circular n° A-130.

counter-terrorism, individuals may also lodge a complaint with the officers within the law enforcement authorities[34].

Moreover, a number of judicial redress avenues may be used against a public authority or one of its officials, where these authorities process personal data. These avenues of redress[35] are open to all individuals irrespective of their nationality, subject to any applicable conditions.

Generally speaking, under the provisions relating to judicial review contained in the regulations on administrative procedure[36], 'any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action' is entitled to seek judicial review. This includes the possibility of asking the court to 'hold unlawful and set aside agency action, findings, and conclusions found to be […] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law'.

In addition, and more specifically, the regulations relating to the confidentiality of electronic communications[37] set out a system of statutory privacy rights and as such governs law enforcement access to the contents of wire, oral or electronic communications stored by third-party service providers. Unlawful (i.e. not authorised by court or otherwise permissible) access to such communications is punishable and an affected individual can seek redress by filing a civil action in a U.S. federal court for actual and punitive damages as well as equitable or declaratory relief against a government official who has wilfully committed such unlawful acts, or against the United States.

Secondly, several other regulations[38] give data subjects the right to bring an action against a U.S. authority or official regarding the processing of their personal data.

Finally, under the rules on Freedom of Information Act[39], any person has the right to obtain access to federal agency records, including where these contain the individual's personal data. After exhausting administrative remedies, a data subject may invoke such a right to access in court unless those records are protected from public disclosure by an exemption or special law enforcement exclusion. In this case, the court determines whether a derogation applies or has been lawfully invoked by the authority concerned.

4.2 Access for national security purposes

4.2.1 Applicable law, safeguards in place

The collection by the U.S. authorities for national security purposes of personal data transferred from Switzerland to certified U.S. organisations is subject to specific conditions and guarantees. Particular attention should be paid to elements relating to signals intelligence, which involves the collection of electronic communications and data from information systems that may contain personal data.

---

[34] See Title 42 chapter 21E of the United States Code.

[35] See in particular the regulations relating to administrative procedure and freedom of information (see Title 5 of the United States Code) as well as the regulations relating to the confidentiality of electronic communications (see Title 18 of the United States Code).

[36] See Title 5 of the United States Code.

[37] See Title 18, Part I, Chapter 121 of the United States Code.

[38] This is particularly the case for regulations relating to wiretapping and computer fraud and abuse (see Title 18 of the United States Code).

[39] See Title 5 of the US Code.

Bericht

In accordance with Executive Order 12333 of 1981[40] relating to the activities of the United States intelligence services, personal data may be collected outside the United States and therefore also when such data are being transferred from Switzerland to the United States.

In addition, once personal data have been received by certified organisations in the United States, the intelligence services may request access to these data if the regulations in force so authorise. Such data collection may be authorised under the Foreign Intelligence Surveillance Act (FISA)[41].

On 7 October 2022, the President of the United States issued Executive Order 14086[42] on strengthening safeguards for signals intelligence activities; this order largely replaces[43] Presidential Policy Directive 28 (PPD-28)[44]. This order applies to all signals intelligence activities, i.e. it covers both FISA-based activities and those based on Executive Order 12333; its provisions are binding on the entire U.S. intelligence community. It lays down limits and guarantees in addition to those provided by FISA and Executive Order 12333, and also establishes a new redress mechanism enabling these guarantees to be invoked and enforced. The intelligence agencies have updated their policies and procedures to bring them in line with the provisions of Executive Order 14086; after a process involving various consultations, in particular with the Attorney General, the ODNI CLPO and the PCLOB, these policies and procedures were published on 3 July 2023[45].

Executive Order 14086 sets out a catalogue of requirements that apply to all signals intelligence activities. These activities must be based on regulations or presidential authorisation and must be carried out in accordance with the laws of the United States, in particular the U.S. Constitution. Appropriate safeguards must be put in place to take account of the protection of privacy and civil liberties of all individuals, irrespective of nationality or place of residence, when planning activities. In particular there is a need to establish that, on the basis of a reasonable assessment of all the relevant factors, the activities are necessary to advance a valid intelligence priority. In addition, these activities must be carried out in a way that is proportionate to a valid intelligence priority for which they have been authorised. Consideration must be given to whether the importance of the activity to the valid priority outweighs its impact on the privacy and civil liberties of the data subject.

The above requirements are reinforced by safeguards to ensure that interference with the rights of data subjects is limited to what is necessary and proportionate to achieve a legitimate aim.

Firstly, the order limits the grounds on which data may be collected as part of signals intelligence activities. On the one hand, the order defines the legitimate objectives that may be pursued, such as understanding or assessing the capabilities, intentions or activities of foreign organisations, including international terrorist organisations, that pose an actual or potential threat to the national security of the United States. On the other, the order lists certain objectives that must never be pursued, for example those that hinder the free expression of political ideas or opinions by individuals or the press. Furthermore, actual collection can only take

---

40 See Executive Orders | National Archives.

41 See Title 50 Chapter 36 of the US code.

42 See links to reference texts at the end of the document.

43 Executive Order 14086 replaces PPD-28 except for certain specific articles (partial revocation of PPD-28).

44 See Presidential Policy Directive -- Signals Intelligence Activities | whitehouse.gov (archives.gov).

45 See INTEL - ODNI Releases IC Procedures Implementing New Safeguards in Executive Order 14086.

place to advance an intelligence priority; priorities are established by the Director of National Intelligence and assessed by the ODNI's CLPO, and then submitted to the President of the United States for approval. This procedure ensures that privacy aspects are taken into account when intelligence priorities are set.

Secondly, once an intelligence priority has been established, the requirements govern the decision as to whether and to what extent signals intelligence can be collected to further that priority. These requirements put into specific terms the general standards of necessity and proportionality set out in the order. Thus signals intelligence may only be gathered after it has been determined, on the basis of a reasonable assessment of all relevant factors, that collecting intelligence is necessary to advance a specific intelligence priority. In determining necessity, intelligence agencies should consider the availability, feasibility and validity of other less intrusive sources and methods and, where available, priority should be given to these other less intrusive sources and methods.

Where collecting intelligence is deemed necessary, it must be as targeted as possible. In order to prevent a disproportionate impact on privacy and civil liberties, i.e. to strike a fair balance between the needs of national security and the protection of privacy and civil liberties, all relevant factors must be duly taken into account, such as the nature of the objective pursued; the intrusiveness of collection, including its duration, the likely contribution of the collection to the purpose pursued, the reasonably foreseeable consequences for the data subjects, and the nature and sensitivity of the data to be collected.

Bulk collection of signals intelligence, i.e. the collection of large quantities of signals intelligence without, for example, using specific selection criteria[46], can only take place outside the United States, on the basis of Executive Order 12333. However, priority must be given to targeted collection. Under Executive Order 14086, bulk collection is only permitted where the information necessary to advance a validated intelligence priority cannot reasonably be obtained through targeted collection, and specific safeguards apply: methods and technical measures must be applied to limit the data collected to what is necessary to advance a validated intelligence priority, while minimising the collection of non-pertinent information; the use of information collected in bulk is limited to six defined purposes, including protection against terrorism and protection against foreign espionage, sabotage or assassination. Finally, any querying of signals intelligence obtained in bulk may only take place where necessary to advance a validated intelligence priority, in pursuit of these six objectives and in accordance with policies and procedures that appropriately take into account the impact of the queries on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

In addition to the requirements of Executive Order 14086, the signals intelligence collection of data that has been transferred to an organisation in the United States is subject to specific limitations and safeguards governed by Section 702 FISA, according to which the Attorney General and the Director of National Intelligence submit annual certifications to the Foreign Intelligence Surveillance Court (FISC) which identify categories of foreign intelligence information to be acquired. Certifications must be accompanied by targeting, minimisation and querying procedures, which are also approved by the Court and are legally binding on intelligence agencies.

[46] Bulk collection, however, differs from generalised and indiscriminate collection (‘mass surveillance’) without limitations or safeguards.

Bericht

The FISC is an independent tribunal whose decisions can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR) and, ultimately, the Supreme Court of the United States[47]. The FISC is supported by a standing panel of five attorneys and five technical experts who have expertise in national security matters and civil liberties, thus ensuring that privacy considerations are properly taken into account.

Individual targeting decisions are made by the National Security Agency *(NSA*) in accordance with FISC-approved targeting procedures, which require the NSA to assess, based on the totality of the circumstances, whether targeting a specific person is likely to acquire a category of foreign intelligence information identified in a certification. Targeting is carried out by choosing selectors that identify specific means of communication, such as a target's e-mail address or telephone number, rather than keywords or the names of targeted individuals. The NSA must document the factual basis for the selection of the target and, at regular intervals after the initial targeting, confirm that the targeting standard continues to be met, otherwise collection must be stopped. The selection by the NSA of each target and its record of each targeting assessment and rationale is reviewed every two months by the intelligence oversight offices at the DoJ, who are under an obligation to report any violation to the FISC and to Congress.

As regards the other legal bases for collecting personal data transferred to certified organisations in the U.S., different limitations and safeguards apply. In general, the collection of data in bulk is specifically prohibited and the use of specific selectors is required. To conduct individualised electronic surveillance, intelligence agencies must submit an application to the FISC with a statement of the facts and circumstances relied upon to justify the belief that there is probable cause that the facility is used or about to be used by a foreign power or an agent of a foreign power. The FISC will assess, among other issues, whether on the basis of the submitted facts there is probable cause that this is indeed the case. An application for an order must also be submitted to the FISC in order to carry out a search of premises or property that is intended to result in an inspection or seizure of information, material, or property or for the installation of pen registers or trap and trace devices.

The processing of personal data collected by U.S. intelligence agencies through signals intelligence is also subject to a number of safeguards. First of all, each intelligence agency must ensure appropriate data security and prevent access by unauthorised persons to personal data collected through signals intelligence. Access to collected data must be limited to authorised, trained personnel with a need to know the information to perform their mission. More generally, intelligence agencies must provide appropriate training to their employees. Furthermore, intelligence agencies must comply with Intelligence Community standards for accuracy and objectivity, in particular with regard to ensuring data quality and reliability, the consideration of alternative sources of information, and objectivity in performing analyses. In addition, the data retention periods apply regardless of the nationality of the data subjects. Moreover, specific rules apply as regards the dissemination of personal data collected through signals intelligence. For example, personal data may not be disseminated solely because of a person’s nationality or country of residence or for the purpose of circumventing the requirements of Executive Order 14086. Lastly, in order to facilitate oversight of compliance with the applicable legal requirements as well as effective redress, each intelligence agency is required to keep appropriate documentation about the collection of signals intelligence. In addition to the abovementioned safeguards of Executive Order 14086 for the use of information collected

[47] See Title 50 Chapter 36 of the United States Code.

through signals intelligence, the intelligence agencies are subject to more general requirements on purpose limitation, data minimisation, accuracy, security, retention and dissemination, following in particular from Committee on National Security Systems instruction (CNSSi) 1253, *Security Categorization and Control Selection for National Security Systems*, the United States Office of Management and Budget (OMB) Circular No. A-130 and other applicable regulations.

4.2.2 Independent authority, redress

4.2.2.1 Oversight

The activities of the intelligence agencies are subject to supervision by different bodies. Firstly, Executive Order 14086 requires each intelligence agency to have senior-level legal, oversight and compliance officials to ensure compliance with the applicable national law. In particular, they must conduct periodic oversight of signals intelligence activities and ensure that any non-compliance is remedied. Intelligence agencies must provide these officials with access to all relevant information to carry out their oversight functions and may not take any actions to impede or improperly influence their oversight activities. Moreover, any significant non-compliance incident identified by an oversight official or any other employee must be promptly reported to the head of the intelligence agency and the Director of National Intelligence, who must ensure that any necessary actions are taken to remediate and prevent the recurrence of the incident of non-compliance.

As is the case in relation to criminal law enforcement authorities, Civil Liberties Protection Officers (CLPOs) exist at all intelligence agencies[48]. The powers of these CLPOs typically encompass the supervision of procedures to ensure that the respective department/agency is adequately considering privacy and civil liberties concerns and has put in place adequate procedures to address complaints from individuals who consider that their privacy or civil liberties have been violated. The heads of intelligence agencies must ensure that CLPOs have the resources to fulfil their mandate, are given access to any material and personnel necessary to carry out their functions, and are informed about and are consulted on proposed policy changes. The CLPOs report regularly to Congress and the PCLOB, including on the number and nature of the complaints received by the department/agency with a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out.

In addition, each intelligence agency has an independent inspector general whose responsibilities include overseeing foreign intelligence activities. Within the ODNI, the Office of the Inspector General of the Intelligence Community has comprehensive jurisdiction over the entire Intelligence Community. These inspectors general are independent and responsible for conducting audits and investigations relating to the programmes and operations carried out by the agency concerned for national intelligence purposes, including with regard to any abuse or violation of the law. They have access to all records, reports, audits, reviews, documents, papers, recommendations or other relevant material, if needed by subpoena, and may take testimony. Inspectors general refer cases of suspected criminal violations for prosecution and make recommendations for corrective action to agency heads. While their recommendations are non-binding, their reports, including on follow-up action (or the lack thereof) are generally made public and sent to Congress, which can on this basis exercise its own oversight function.

[48] See Title 42 of the US Code.

Moreover, the Intelligence Oversight Board (IOB), which is established within the President's Intelligence Advisory Board (PIAB), oversees compliance by the intelligence authorities with the Constitution and all applicable rules. The PIAB comprises 16 members appointed by the President from outside the U.S. government. The IOB comprises a maximum of five members designated by the President from among PIAB members. Under Executive Order 12333, the heads of all intelligence agencies are required to report any intelligence activity for which there is reason to believe that it may be unlawful or contrary to an executive order or presidential directive to the IOB. The IOB is in turn required to inform the President about intelligence activities it believes may be in violation of national law (including executive orders) and are not being adequately addressed by the Attorney General, Director of National Intelligence or the head of an intelligence agency. In addition, the IOB is required to inform the Attorney General about possible criminal law violations.

Furthermore, intelligence agencies are subject to oversight by the PCLOB. According to its founding statute, the PCLOB is entrusted with responsibilities in the field of counter-terrorism policies and their implementation, with a view to protecting privacy and civil liberties. In its review of intelligence agencies actions, it can access all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, and may take testimony from witnesses. It may issue recommendations to the government and intelligence agencies, and regularly reports to congressional committees and the President. Reports of the Board, including the ones to Congress, must be made publicly available to the greatest extent possible. The PCLOB is also charged with carrying out specific oversight functions as regards the implementation of Executive Order 14086, in particular by reviewing whether agency procedures are consistent with the Order and evaluating the correct functioning of the redress mechanism (see Section 4.2.2.2).

In addition to the oversight mechanisms within the executive branch, specific committees in the U.S. Congress (the House and Senate Intelligence and Judiciary Committees) have oversight responsibilities regarding all U.S. foreign intelligence activities. Members of these committees have access to classified information as well as intelligence methods and programmes. The committees exercise their oversight functions in different ways, in particular through hearings, investigations, reviews and reports. The congressional committees receive regular reports on intelligence activities, including from the Attorney General, the Director of National Intelligence, intelligence agencies and other oversight bodies (e.g. inspectors general).

More generally, the U.S. Intelligence Community undertakes various efforts to provide transparency about its intelligence activities. For example, in 2015, the ODNI adopted Principles of Intelligence Transparency and a Transparency Implementation Plan[49]. In this context, the Intelligence Community has made and continues to release declassified parts of policies, procedures, oversight reports, etc.

Finally, the collection of personal data pursuant to FISA is also subject to oversight by the FISC. Where necessary, the FISC may order the relevant intelligence agency to take remedial action. The remedies in question may range from individual to structural measures, e.g. from terminating data acquisition and deleting unlawfully obtained data to a change in the collection practice. Moreover, during its annual review of certifications, the FISC considers non-compliance incidents to determine if the submitted certifications comply with FISA require-

[49] See the Principles of Intelligence Transparency for the IC (dni.gov).

ments. Similarly, if the FISC finds that the government's requested FISA section 702 certifications were not sufficient, including because of particular compliance incidents, it may issue a 'deficiency order' requiring the government to remedy the violation within 30 days or requiring the government to cease or not begin implementing the certification. The FISC assesses any compliance issues it identifies and may require changes to procedures or additional oversight and reporting to address these issues.

4.2.2.2 Redress

Opportunity to bring legal action before an independent and impartial tribunal is offered, allowing data subjects to have access to their personal data, to have the lawfulness of government access to their data reviewed and, if a violation is found, to have that violation remedied, including through the rectification or deletion of their personal data.

A specific redress mechanism is established under Executive Order 14086, complemented by the Regulation on the Data Protection Review Court (DPRC) issued by the Attorney General on 7 October 2022, to handle and resolve complaints from individuals concerning U.S. signals intelligence activities. Any data subject in Switzerland is entitled to submit a complaint to the redress mechanism concerning an alleged violation of U.S. law governing signals intelligence activities that adversely affects their privacy and civil liberties interests. This redress mechanism is available to individuals from countries or regional economic integration organisations that have been designated by the U.S. Attorney General. On 7 June 2024, Switzerland was designated as a qualifying state with regard to the redress mechanism[50].

A data subject in Switzerland who wishes to file a complaint must submit it to the FDPIC as the independent authority for overseeing data protection in Switzerland and the appropriate public authority to transmit complaints under the redress mechanism. This procedure ensures easy access to the redress mechanism by allowing data subjects to turn to an authority with which they can communicate in their own language. In order to provide a starting point for the redress mechanism to carry out a review, information must be provided to verify the complaint is concerning an individual and certain basic information must be provided regarding the personal data, such as an email address or telephone number, that is reasonably believed to have been transferred to the U.S. and the means by which it is believed to have been transferred; the identities of the U.S. Government entities believed to be involved in the alleged violation (if known); and the nature of the relief sought, such as the deletion of the data concerned. On the other hand, it is not necessary to show that personal data have in fact been collected by intelligence agencies or that they have been subject to U.S. signals intelligence activities. In this context, the FDPIC receives the complaint and simply verifies the individual's identity and checks whether the basic information has been provided. If this is the case, the FDPIC transmits the complaint to the redress mechanism.

The initial investigation of complaints to this redress mechanism is carried out by the ODNI CLPO, whose existing statutory role and powers have been expanded for those specific actions taken pursuant to Executive Order 14086. In addition, Directive 126 of the Intelligence Community[51] issued by the Office of the Director of National Intelligence details the implementation procedures for the intelligence redress mechanism under Executive Order 14086. Within the Intelligence Community, the ODNI CLPO is, inter alia, responsible for ensuring that the protection of civil liberties and privacy is appropriately incorporated in policies and proce-

[50] See links to reference texts at the end of the document.

[51] See links to reference texts at the end of the document.

dures of the ODNI and intelligence agencies; overseeing compliance by the ODNI with applicable civil liberties and privacy requirements; and conducting privacy impact assessments. The ODNI CLPO can only be dismissed by the Director of National Intelligence for cause, i.e. in case of misconduct, malfeasance, breach of security, neglect of duty, or incapacity. When conducting its review, the ODNI CLPO has access to the information for his or her assessment and can rely on the mandatory assistance of CLPOs in the various intelligence agencies. Intelligence agencies are prohibited from impeding or improperly influencing the reviews. This includes the Director of National Intelligence, who must not interfere with the review. When reviewing a complaint, the ODNI CLPO must apply the law impartially, having regard to both the national security interests in signal intelligence activities and privacy protections. In its review, the ODNI CLPO determines whether a violation of applicable U.S. law has occurred and, if that is the case, decides on an appropriate remediation. Remediation involves measures that fully redress an identified violation, such as terminating unlawful acquisition of data, deleting unlawfully collected data, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorisation or that were unlawfully disseminated. Decisions of the ODNI CLPO on individual complaints, including on the remediation, are binding on intelligence agencies concerned, unless the DPRC, discussed below, issues a subsequent contrary decision. The ODNI CLPO must maintain documentation of its review and produce a classified decision explaining the basis for its factual findings, the determination with respect to whether a covered violation occurred and the determination of the appropriate remediation. If the ODNI CLPO’s review reveals a violation of any authority subject to the oversight of the FISC, the CLPO must also provide a classified report to the Assistant Attorney General for National Security, who is in turn under an obligation to report the non-compliance to the FISC, which can take further enforcement action.

Once the review is completed, the ODNI CLPO informs the complainant, through the FDPIC, in a standard response either that 'the review either did not identify any covered violations' or that 'the ODNI CLPO issued a determination requiring appropriate remediation' through the FDPIC. This allows protection of the confidentiality of activities conducted to protect national security, while providing the data subject with a decision confirming that their complaint has been duly investigated and adjudicated. This decision can moreover be challenged by the data subject. To this end, the data subject will be informed of the possibility of appealing to the DPRC for a review of the ODNI CLPO’s determinations and that, in the event that thedata subject appeals to the DPRC, a special advocate will be selected to advocate for the complainant’s interest in the matter and ensure that the DPRC panel is well informed of the issues and the law with respect to the matter.

Any complainant, as well as each element of the Intelligence Community, may seek review of the ODNI CLPO’s decision before the Data Protection Review Court (DPRC). If an element of the Intelligence Community seeks review with the DPRC, a special advocate also will be appointed to advocate for the complainant’s interest in the matter and ensure that the DPRC panel is well informed of the issues and the law with respect to the matter. These applications for review must be submitted within 60 days after receiving notification from the ODNI CLPO that its review is complete and include any information the individual wishes to provide to the DPRC, such as arguments on questions of law. Swiss data subjects must again submit their application through the FDPIC who will then transmit the data subject’s review request to the DPRC.

Bericht

The DPRC is an independent tribunal established by the Attorney General on the basis of Executive Order 14086. It comprises a minimum of six judges, appointed by the Attorney General in consultation with the PCLOB, the Secretary of Commerce and the Director of National Intelligence for renewable terms of four years. The appointment of judges by the Attorney General is informed by the criteria used by the executive branch when assessing candidates for the federal judiciary, giving weight to any prior judicial experience. In addition, the judges must be legal practitioners (i.e. active members in good standing of the bar and duly licensed to practise law) and have appropriate experience in privacy and national security law. The Attorney General must endeavour to ensure that at least half of the judges have prior judicial experience and all judges must hold security clearances to be able to access classified national security information. Furthermore, the judges must not be employees of the executive branch at the time of their appointment or have been so in the preceding two years. Similarly, during their term of office at the DPRC, the judges may not have any official duties or employment within the U.S. Government, other than being judges at the DPRC. The independence of the adjudication process is achieved through a number of guarantees. In particular, the executive branch (the Attorney General and intelligence agencies) is barred from interfering with or improperly influencing the DPRC's review. The DPRC itself is required to adjudicate cases impartially and operates according to its own rules of procedure adopted by majority vote. Moreover, DPRC judges may be dismissed only by the Attorney General and only for cause (i.e. misconduct, malfeasance, breach of security, neglect of duty or incapacity), after taking due account of the standards applicable to federal judges laid down in the Rules for Judicial-Conduct and Judicial-Disability Proceedings[52].

Applications to the DPRC are reviewed by panels of three judges, including a presiding judge, who must act in accordance with the Code of Conduct for U.S. Judges. Each panel is assisted by a Special Advocate, who has access to all information pertaining to the case, including classified information. The role of the Special Advocate is to ensure that the complainant's interests are represented and that the DPRC panel is well informed about all relevant issues of law and fact. When the complainant has filed an application for review, the Special Advocate can seek information from the complainant through written questions, to further inform its position on an application for review to the DPRC by an individual. The DPRC reviews the determinations made by the ODNI CLPO (both whether a violation of applicable U.S. law has occurred and as regards the appropriate remediation) based, at a minimum, on the record of the ODNI CLPO's investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an intelligence agency. A DPRC panel has access to all information necessary to conduct a review, which it may obtain through the ODNI CLPO.

When concluding its review, the DPRC may decide that there is no evidence indicating that signals intelligence activities occurred involving personal data of the complainant, or decide that the ODNI CLPO's determinations were legally correct and supported by substantial evidence, or issue its own determinations if the DPRC disagrees with the determinations of the ODNI CLPO. When the DPRC issues a determination that diverges from the ODNI CLPO's, the DPRC's decision takes precedence and is binding on the ODNI CLPO and intelligence agencies.

In all cases, the DPRC adopts a written decision by majority vote. If the review reveals a violation of the applicable rules, the decision will specify any appropriate remediation, which includes deleting unlawfully collected data, deleting the results of inappropriately conducted

[52] See Executive Order 14086 and the Regulation issued by U.S. Attorney General. See also Data Protection Review Court website, which lists current judges and their backgrounds: https://www.justice.gov/opcl/redress-data-protection-review-court.

queries, restricting access to lawfully collected data to appropriately trained personnel, or recalling intelligence reports containing data acquired without lawful authorisation or that were unlawfully disseminated. The DPRC's decision is binding and final with respect to the complaint before it. Moreover, if the review reveals a violation of any authority subject to the oversight of the FISC, the DPRC must also provide a classified report to the Assistant Attorney General for National Security, who in turn is under an obligation to report the non-compliance to the FISC, which can take further action. Each decision of a DPRC panel is transmitted to the ODNI CLPO. In cases where the DPRC's review was triggered by an application from the complainant, the complainant is notified through the FDPIC that the DPRC has completed its review and that the review either did not identify any covered violations or that the DPRC issued a determination requiring appropriate remediation. The Office of Privacy and Civil Liberties of the DoJ maintains a record of all information reviewed by the DPRC and all decisions issued, which is made available for consideration as non-binding precedent for future DPRC panels. The DoC is also required to maintain a record for each complainant who submitted a complaint. To enhance transparency, the DoC must, at least every five years, contact relevant intelligence agencies to verify whether information pertaining to a review by the ODNI CLPO or a review by the DPRC has been declassified. If this is the case, the individual will be notified, through the appropriate public authority, that such information may be available under applicable law.

Finally, the correct functioning of this redress mechanism will be subject to regular and independent evaluation. More specifically, the functioning of the redress mechanism is subject to annual review by the PCLOB, an independent body[53]. As part of this review, the PCLOB will, inter alia, assess whether the ODNI CLPO and DPRC have processed complaints in a timely manner; whether they have obtained full access to necessary information; whether the substantive safeguards of Executive Order 14086 have been properly considered in the review process; and whether the Intelligence Community has fully complied with determinations. The PCLOB will submit a report on the outcome of its review to the President, Attorney General, Director of National Intelligence, head of intelligence agencies, the ODNI CLPO and congressional intelligence committees, which will also be made public in an unclassified version. The Attorney General, Director of National Intelligence, ODNI CLPO and heads of intelligence agencies are required to implement or otherwise address all recommendations included in such reports. In addition, the PCLOB will make an annual public certification as to whether the redress mechanism is processing complaints consistent with the requirements of Executive Order 14086.

In addition to the specific redress mechanism established under Executive Order 14086, redress avenues are available to all individuals, irrespective of nationality or place of residence, before ordinary U.S. courts. In particular, FISA and a related statute provide the possibility for individuals to bring a civil action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed; to sue U.S. government officials acting in their personal capacity for money damages; and to challenge the legality of surveillance in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the U.S. A more general recourse option is offered by the rules on administrative procedure, according to which 'any person suffering legal wrong because of

[53] Executive Order 14086 encourages the PCLOB to conduct an annual review of the functioning of the redress mechanism. The PCLOB agreed to do these reviews (see Oversight Projects - PCLOB).

agency action, or adversely affected or aggrieved by agency action', is entitled to seek judicial review.

Finally, under the law on freedom of information[54], any person has a right of access to information from federal authorities, including when it contains personal data. Gaining such access can also facilitate bringing proceedings before ordinary courts, including in support of showing standing. Agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations, but complainants who are dissatisfied with the response have the right to challenge it by seeking administrative and, subsequently, judicial review before the federal courts.

5 Other criteria

5.1 International commitments

International commitments must be taken into account. In this respect, data protection commitments are not the only commitments that are relevant and other forms of commitment may be taken into account, for example agreements governing the exchange of information.

The United States is a party to a number of international frameworks that include commitments relating to the right to privacy and human rights in general.

As a member of the Organisation for Economic Co-operation and Development (OECD), the United States participates in the OECD's work on data governance and privacy protection. It has undertaken to comply with the OECD's privacy protection framework, in particular the OECD Privacy Guidelines[55]. The United States also played an active role in drafting the Declaration on Government Access to Personal Data Held by Private Sector Entities[56].

The United States is signatory to the Council of Europe's Budapest Convention on Cybercrime[57].

In addition, the United States is a member of the Asia-Pacific Economic Cooperation (APEC) and a party to the APEC Privacy Framework[58].

The FTC is also an accredited member of the Global Privacy Assembly[59], while the PCLOB and the DoJ's Privacy and Civil Liberties Officer are observers.

Bilateral or plurilateral free trade or e-commerce agreements may also be relevant if they contain provisions relating to the protection of personal data and cross-border data flows. The free trade agreement between the United States, Mexico and Canada and the free trade agreement between the United States and Japan[60] should be mentioned in particular. The

[54] See Tile 5 of the US Code.

[55] Available at the following link: OECD Legal Instruments.

[56] Available at the following link: OECD Legal Instruments.

[57] Available at the following link: CETS 185 - Convention on Cybercrime (coe.int).

[58] Available at the following link: APEC Privacy Framework.

[59] See Global Privacy Assembly.

[60] See Digital Trade & E-Commerce FTA Chapters | United States Trade Representative (ustr.gov).

United States also participates in the negotiations on an e-commerce agreement currently being held on the basis of a joint initiative by WTO members[61].

5.2 Rule of law

The United States is a federal republic comprising 50 states, plus non-state territories. Its form of government is that of a democracy.

Foreign policy, the armed forces, intelligence activities and foreign trade are the responsibility of the federal government. The 50 federal states have powers in a wide range of areas, including justice, education, etc.

The United States Constitution, dating from 1787, is the oldest modern constitution still in force. The Constitution enshrines the separation of powers: legislative power is exercised by a congress composed of two chambers, the Senate and the House of Representatives; executive power is exercised by the President and Vice-President of the United States; the Supreme Court is the highest judicial body in the United States, hearing cases from the lower federal courts as the highest court of appeal, as well as cases involving questions of federal law or interpretation of the Constitution. The independence of the judiciary is guaranteed by the Constitution.

5.3 Human rights

Furthermore, the criterion relating to respect for human rights must be seen in relation to a state's overall legal framework, particularly as regards protection against any disproportionate interference with privacy.

The U.S. Constitution sets out certain fundamental rights that cannot be violated by federal or state authorities and which are enforced by the judiciary. These rights in part mirror the human rights contained in the Universal Declaration of Human Rights[62]. These include freedom of expression, freedom of belief, freedom of assembly, equality and procedural guarantees.

Additionally, Supreme Court rulings have addressed the protection of privacy interests in a number of contexts, including in particular in the context of the Fourth Amendment, which establishes a right against unreasonable searches and seizures by the government[63].

6 Conclusion

It follows from the foregoing that when U.S. law enforcement and national security authorities access personal data transferred from Switzerland to certified organisations, such access is governed by a legal framework that lays down the conditions under which access can take place and ensures that access and further use of the data are limited to what is necessary and proportionate to the public interest objective pursued. These safeguards can be invoked by individuals thanks to the redress offered and are therefore effective.

On the basis of the foregoing review, the FOJ therefore concludes that the United States provides an adequate level of protection for personal data transferred under the Swiss-U.S. DPF

---

61 See WTO | Joint Initiative on E-Commerce.

62 Accessible at the following link: The Universal Declaration of Human Rights.

63 See *Griswold v. Connecticut, 381 US 479 (1965),* accessible at the following link: Griswold v. Connecticut : 381 US 479 (1965): Justia US Supreme Court Center.

from a data controller or processor in Switzerland to certified organisations in the United States.

In the event of a positive decision by the Federal Council on the basis of this assessment, data transfers between data controllers or processors in Switzerland and certified organisations in the United States may take place without the need to obtain additional guarantees, in accordance with the provisions of Article 16 paragraph 1 FADP.

Links to reference texts:

- Principles, including supplemental principles, of the trade framework between Switzerland and the United States on data protection for certified organisations, letters to confirm the commitments made drawn up by the following authorities: Department of Justice (DoJ), Department of Commerce (Secretary of Commerce) (DoC), International Trade Administration (ITA), Federal Trade Commission (FTC) and Department of Transportation (DoT), as well as a letter from the Office of the Director of National Intelligence (ODNI) to the DoC: https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3
- Executive Order 14086 of 7 October 2022: https://www.state.gov/executive-order-14086-policy-and-procedures
- Regulation on the Data Protection Review Court issued by U.S. Attorney General on October 7, 2022: https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court
- Intelligence Community Directive 126 issued by the ODNI on 6 December 2022: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Recourse-Mechanism.pdf
- Designation of Switzerland on 7 June 2024 as a state benefiting from the two-tier appeal mechanism, including access to the Data Protection Review Court: https://www.justice.gov/opcl/media/1355326/dl?inline, see also: https://www.justice.gov/opcl/executive-order-14086