32nd Annual Report 2024/2025

Federal Data Protection and Information Commissioner

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Annual Report 2024/2025

Federal Data Protection and Information Commissioner

The FDPIC shall submit a report on his or her activities to the Federal Assembly every year. He or she shall submit the report to the Federal Council at the same time. The report shall be published (Art. 57 FADP).

This report covers the period between 1 April 2024 and 31 March 2025 for the section on data protection. For the section on freedom of information it corresponds to the calendar year 1 January to 31 December 2024.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The primacy of politics and language

With artificial intelligence accessible to everyone, digitalisation has produced its latest machine wonder, which leaves us marvelling at its ability to write, speak, sing or paint autonomously.

However, those who simply 'marvel' at these achievements risk falling behind in our digital society. Digital literacy for all is the key to preventing this—a message echoed across the media. The same message is driven home by data protection authorities, which explain how we can prevent tracking, the sharing of location data and the feeding of our personal data into artificial intelligence systems, and for good reason.

It is certainly reasonable to expect politicians to familiarise themselves with the realities of an increasingly digital world. However, calling for proof of digital literacy as a prerequisite for holding political office would be a step too far: the representatives of the people are perfectly capable of weighing up the risks and opportunities presented to society by digital technologies. But they must be able to rely on those who fully understand these technologies and their complex application environments to be both willing and able to share their knowledge in clear, comprehensible language.

Therefore, the federal data protection supervisory authority has been persistent in its efforts during the year under review to ensure that the Administration presented the privacy-related risks of its digitalisation projects in clear, comprehensible language in its proposals to the Federal Council and in its dispatches to Parliament.

Adrian Lobsiger
Federal Data Protection and Information Commissioner

Bern, 31st March 2025

Freedom of Information

The FDPIC

Current Challenges

I Data protection

Western democratic societies possess sufficient digital technology, financial resources and manpower to expand their control infrastructures in such a way that the private and self-determined lives of their citizens, as guaranteed by liberal constitutions, are turned into their opposite. Drones and sensors are cheap and can be manufactured in almost unlimited numbers and used for blanket surveillance of individuals' every move and facial recognition in public spaces. All this can be combined with the networking of all government information systems and hi-tech digital surveillance of online activities by the state and the digital economy through to AI-supported social scoring. As a result, the daily lives of people in the West would be subjected to almost constant surveillance.

The technology-neutral Swiss Federal Act on Data Protection (FADP) bans the use of blanket facial-recognition surveillance and social scoring, although the Commissioner can only derive this ban by interpreting the Act as the ban is not explicitly enshrined in the latter like it is in the EU's AI Act (see our statement of 9 November 2023). Data protection law and supervisory authorities such as the FDPIC play an important role in ensuring that Western democracies do not blindly succumb to the sweet poison of technological feasibility. Data protection itself is founded on constitutional guarantees of freedom and the general legal conviction that these guarantees must be respected and enforced by independent institutions of the democratic constitutional state.

Meanwhile, in more than a few of Switzerland's Western partner states, there is a growing rift between supporters of the rule of law and those who allegedly have nothing to hide and therefore reject fundamental rights and data protection for themselves as unnecessary and patronising, and for others as an imposition by an out-of-touch bureaucracy which seems to prefer to protect 'offenders' rather than citizens. Often driven by resentment against 'elites', these groups react with particular incomprehension when courts and supervisory authorities scrutinise the actions of the executive.

With the repetitive criticism of the rule of law and an ever-widening gap in opinions, a way of thinking characterised by an unquenchable thirst for security is taking hold in the Western communities concerned. A cognitive model that would like to see all control infrastructures upgraded to the extent that is technologically feasible and that welcomes the restrictive consequences of digital social monitoring for 'criminals', 'strangers' and dissenters while ignoring them for themselves and for like-minded people. Where this kind of mindset establishes itself as the dominant culture in the West, the individuals living there can expect to exist as objects of an informational regime controlled by external forces right down to their private lives, and sooner rather than later.

«The FADP prohibits comprehensive facial recognition and digital social control.»

II Freedom of information

Processing time for applications for access to documents and mediation proceedings

Growing interest in freedom of information has led to an increase in the number of applications for access to documents of the Administration.

The same applies to the FDPIC's mediation proceedings: 2024 saw a record number of mediation requests, which affected the length of time required to complete the mediation proceedings. During the year under review, the FDPIC was only able to meet the statutory processing time of 30 days in just over a quarter of all proceedings (see Section 2.3). Another factor that contributed to longer proceedings was the increased complexity of the legal issues involved. For example, questions regarding the scope of application of the Freedom of Information Act sometimes require extensive clarification before a situation can be assessed. Mediation procedures also tend to take longer when legal representatives are involved, be it by the applicant, by third parties or by the Administration.

With interest in accessing official documents set to continue growing, along with the number of mediation requests, completing mediation proceedings within the required time frame is likely to remain a challenge.

Number of special exemptions to the FoIA grows

This reporting year saw further efforts by the Administration to exclude more areas of its activities and certain categories of documents from the Freedom of Information Act. In the various office consultations, the FDPIC took a critical view of the matter as reservations undermined the principle of freedom of information and the transparency within the Administration that the principle sought to achieve. Whether or not a legal provision takes precedence as a special provision under Article 4 of the Freedom of Information Act needs to be determined for the case at hand by interpreting the relevant rules.

In light of the growing number of special FoIA exemptions, the FDPIC has published a table providing an up-to-date overview of all exemptions (see Section 2.5) – as in the last annual report – which can also be found on the FDPIC's website.

«In 2024, more mediation requests were received than ever before.»

III National and international cooperation

Co-operation on a national level

The federal, cantonal and communal data protection authorities continue to strengthen cooperation in order to ensure effective and comprehensive oversight.

The FDPIC and his data protection counterparts continued their discussions on the demarcation of responsibilities in data protection, in particular the question as to when federal or cantonal legislation applies (see 31st Annual Report, Section III). Differences were discussed for example with reference to employment relationships at private institutions that delegate public tasks or have service contracts with a canton or cantonal public institutions. These discussions took place in the public transport sector and in the health and social care sector, for example in relation to nursing homes.

The data protection authorities also held regular discussions on the introduction and/or operation of shared-database platforms. These required a more in-depth legal and technical analysis, specifically concerning the clear demarcation of roles and responsibilities. This is the case, for instance, where the Confederation operates a platform that processes personal data originating from the cantons in accordance with cantonal legal obligations. Examples include the POLAP (see Section 1.2), Justitia (see Section 1.1) and online voting (see Section 1.1) projects. As part of the POLAP project, the FDPIC and privatim also issued a position paper (FDPIC, 27.03.2024; privatim, 23.02.2024).

Exchange with privatim

Finally, as an associate member, the FDPIC took part in privatim's meetings, which provided an opportunity to discuss current issues such as clouds and the legal consequences of data protection and security breaches.

Annual discussions with federal data protection officers

For the second year running, the FDPIC held a briefing session for federal data protection officers. As the first point of contact, they are regularly in contact with the FDPIC. It is therefore important that the federal data protection officers are kept fully informed of new developments in data protection – legal, technical or practical aspects – particularly with regard to the discharge of their legal duties. This event is also an opportunity for them to meet their colleagues and discuss the day-to-day challenges of their role.

Annual meetings with data protection associations in Switzerland

As every year, the FDPIC met with data protection associations to discuss current challenges. Gaining insight into the realities of private companies is crucial as it allows for an exchange on their practices and challenges. These exchanges also enable the FDPIC to identify the priorities and interests of the different language regions.

International cooperation

International exchanges remain of crucial importance in view of the presence of global technology companies in the Swiss market and the associated enforcement issues with a cross-border character.

The FDPIC maintains his presence on important international committees. Of primary importance for the Commissioner is the exchange with data protection authorities in the EU and the EEA. During the reporting year, he was equally interested in the informal meetings of the states that have an adequacy decision with the EU (so-called 'Adequacy Groups'), to which the EU on the one hand and the data protection authority of the United Kingdom on the other hand invited.

Data protection


Timer
6:58
Samstag, 18. Januar

1.1 Digitalisation and fundamental rights

CONSULTANCY

The CEBA project of the Federal Chancellery

During the year under review, the FDPIC continued to monitor the Cloud Enabling Office Automation (CEBA) project from a supervisory perspective. In particular, he focused on reviewing the data protection impact assessment prepared by the Federal Administration and overseeing the first training sessions for federal staff.

Launched in 2019, the Cloud Enabling Office Automation (CEBA) project is managed by the Digital Transformation and ICT Steering (DTI) Sector of the Federal Chancellery (FC). The aim is to replace the Microsoft Office LTSC Professional Plus 2021 product suite currently in use on the Federal Administration's workstation systems with the cloud-based Microsoft Office 365 (M365) system. The DTI Sector involved the FDPIC early on in the project, and we were therefore able to inform the public about the plan to outsource to the public cloud in the last reporting period (see 31st Annual Report, Section 1.1, and the short news of 7 March 2023).

Since the project was launched, the FDPIC has managed, among other things, to convince the DTI Sector to evaluate medium-term alternatives to Microsoft Office 365. In his supervisory role, he is currently focusing on reviewing and clarifying the data protection impact assessment (DPIA) prepared by the DTI Sector and overseeing the first staff training sessions.

The FDPIC demands that the proportionality of a cloud-based federal solution be assessed and that privacy risks – with particular regard to access by foreign authorities and dependency on market-dominating cloud providers – be analysed and evaluated. We commented on the regular updates to the DPIA and urged for a more detailed description of the main risks and a clearer definition of the necessary risk mitigation measures. The DTI Sector is currently working on these clarifications and additions. At the same time, independent audits are being carried out, the results of which will also be incorporated in the next version of the DPIA.

One key strategy for minimising risks in the CEBA project is the classification of documents containing sensitive personal data, which should continue to be processed in the Federal Administration's own data centres. Federal staff need to be trained accordingly. We attended the first training sessions to ensure compliance with data protection and security requirements. As a federal authority that is administratively affiliated to the Federal Chancellery, the FDPIC will also be availing itself of these migration services and the corresponding training in the future.

DIGITAL PUBLIC SERVICES SWITZERLAND (DPSS)

New duties raise legal questions

Digital Public Services Switzerland has recently taken over all the operational activities of the Swiss Conference on Informatics (SIK/CSI). The FDPIC and the cantonal data protection authorities clarify their cooperation with the DPSS with regard to their respective federal responsibilities.

During the year under review, the operational activities of the Swiss Conference on Informatics (SIK/CSI) were transferred in full to Digital Public Services Switzerland (DPSS), which is also jointly supported by the Confederation and the cantons. As a result, the DPSS has also taken over the declarations of conditions with information and communication technology (ICT) providers. In addition, it is now the majority shareholder of eOperations Schweiz AG.

This has raised questions for the FDPIC and the cantonal data protection authorities regarding the legal nature of Digital Public Services Switzerland and the resulting legal consequences and division of responsibilities. One question, for example, is whether the DPSS – as a simple partnership with no legal personality constituted under the Swiss Code of Obligations and based on the framework agreement under public law that determines the performance mandate of the DPSS – qualifies as a public body or as a public federal body within the meaning of the FADP.

ELECTORAL FRAUD

Unethical signature collection

As a result of various media articles and reports from citizens, the FDPIC, in his capacity as the supervisory authority, looked into the case of alleged falsification of signatures and dubious signature collecting methods in connection with popular initiatives and referendums.

In particular, the FDPIC analysed the data protection issues relating to political rights as provided for by law. He looked at who had access to the data and the purposes for which the data was processed when signatures were collected. Based on the information currently available to the FDPIC, it appears that this is not a data protection issue: it would appear that the alleged fraud involves fabricated signatures or addresses as well as signatories who no longer existed. This rules out any possible link with an identified or identifiable natural person and means that the information in question does not constitute personal data and that the Federal Act on Data Protection therefore does not apply in this case.

E-VOTING

Clearly defined responsibilities

The cantons are responsible for monitoring compliance with data protection regulations in online voting.

The Confederation and cantons have been running the e-voting project since 2004. In its decision of 26 June 2019, the Federal Council instructed the Federal Chancellery (FCh) to work with the cantons to redesign the online voting trials. The joint final report on the redesign and resumption of the trials called for a revision of the legal basis for online voting. The partially revised Ordinance on Political Rights (PoRO) and the fully revised Federal Chancellery Ordinance on Electronic Voting (OEV) came into force on 1 July 2022. Article 14 OEV stipulates that the cantons bear overall responsibility for running ballots with electronic voting correctly.

The role of the Confederation and the Federal Chancellery in the project is to grant the cantons a basic licence for trialling online voting (Art. 27a to 27q PoRO). The Confederation and the cantons jointly maintain a set of measures designed to ensure state-of-the-art security for the online voting system. This set of measures is constantly reviewed, adapted and published and outlines plans for further development of the online voting system and any further action required.

The Federal Chancellery is also responsible for reviewing the systems used for online voting. The system currently in use is the Swiss Post e-voting system. Each canton can decide for itself whether or not to use this system. Four cantons currently have a licence to conduct online voting, namely St. Gallen, Basel-Stadt, Thurgau and the Grisons.

The Federal Chancellery only acts as a certification body for online voting: the cantons are responsible for ensuring the security of the systems used and monitoring compliance with data protection regulations.

E-ID

FDPIC involved in preparing the draft e-ID Act

This reporting year, the FDPIC continued to provide supervisory support in the work on the draft e-ID Act. In particular, he continued to advocate the principle of non-traceability of the e-ID in order to ensure additional privacy protection. Non-traceability refers to the unlinkability of different transactions carried out using an e-ID.

During the revision of the e-ID Act, the FDPIC had expressed concern that the creation of an e-ID should not lead to excessive collection of personal data in the digital world. Accessing all of the data in a customer's e-ID merely to check their age, for example in connection with a simple online purchase of products intended for adults only (e. g. alcohol), would be considered excessive and therefore improper. A simple acknowledgement that an individual is over 18 would suffice.

For this reason, the FDPIC continued to advocate the principle of non-traceability for the e-ID in order to ensure additional privacy protection by preventing access to unnecessary data. He called for the principle to be applied in a binding manner when the e-ID was implemented. The authorities accepted his request and included the principle of non-traceability in the Act, which was adopted by Federal Parliament on 20 December 2024.

ELECTRONIC JUSTICE

Justitia 4.0 project of the Confederation and cantons

The FDPIC is overseeing the development of the justitia.swiss platform, which will allow digital communication in the justice system.

justitia.swiss is an online platform that will allow digital communication between all parties involved in judicial proceedings, namely the judicial authorities, lawyers and other parties to proceedings. The purpose of the platform is to implement electronic legal correspondence and access to electronic documents.

During the year under review, at the request of the cantons, the FDPIC was involved in establishing a standardised framework for the pilot projects planned by the cantons and the Confederation, some of which are already underway, while ensuring that the platform is operated in compliance with data protection rules.

The justitia.swiss platform is scheduled to become fully operational in 2026 at the earliest, after the current legal, technical and organisational issues have been resolved. In agreement with the cantons, the FDPIC has taken on coordination of the data protection aspects of the project together with the Federal Office of Justice and the justitia.swiss project organisers.

Under the Federal Act on the Platforms for Electronic Communication in the Justice System (ECJA), which is scheduled to come into force on 1 January 2026 at the earliest, the FDPIC will become the sole data protection supervisory authority for the justitia.swiss platform. At present, preliminary checks on the justitia.swiss pilot operations underway in the individual cantons are still the remit of the cantonal data protection supervisory authorities. However, the aim is for supervisory authority to pass to the FDPIC as quickly as possible, by bringing into force the necessary provisions of the BEKJ at an early stage. This will enable a standardised pilot test to be carried out by the federal authorities and supervised by the FDPIC.

CYBERCRIME

Cyberattack on OneLog

A cyberattack on 24 October 2024 left the OneLog login platform out of operation for about a week. In order to ensure the data security of the numerous users, the FDPIC is being constantly updated by the data controllers on the action already taken and further measures planned.

OneLog's data protection officer informed the FDPIC on 25 October 2024 that the OneLog login platform had been hacked. The FDPIC subsequently received further voluntary notifications from the data controllers and is being constantly updated by them on new findings regarding the incident. According to the FDPIC's guidelines on reporting data security breaches and informing

data subjects in accordance with Article 24 FADP, voluntary reporting occurs when the controller does not recognise a high risk for the data subjects as part of the risk assessment but wishes to notify the FDPIC of the data security breach for other reasons (see text on the reporting of data security breaches in the Focus section). Voluntary reporting makes sense and is useful for all parties involved from a public interest perspective, for example, particularly in cases in which the risk analysis has identified a low risk based on the data affected, albeit one that could spark media interest given the large number of people affected.

OneLog is a login service provided by the Swiss Digital Alliance, an association of several Swiss media companies. The Alliance launched its project to create a central login solution in a pilot phase in spring 2021. The FDPIC reported on this in his 28th Annual Report (Section 1.1).

CYBER ATTACK

Closure of informal preliminary investigations into Concevis AG and the Federal Statistical Office (FSO)

The FDPIC has closed the preliminary investigations into Concevis and the Federal Statistical Office. No serious breaches were found, and the hackers are unlikely to have been able to read the data targeted by the attack. Nevertheless, the FDPIC has identified a number of points that need to be improved.

In November 2023, the software company Concevis fell victim to a ransomware attack. The data affected by the attack included data from the Federal Statistical Office (FSO). Therefore, the FDPIC opened an informal preliminary investigation into Concevis and another into the FSO (see 31st Annual Report, Section 1.2).

Following the preliminary investigation, the FDPIC concluded that it was not necessary to open a formal investigation within the meaning of Article 49 FADP as no serious breaches had been found. Furthermore, the data affected by the cyber-attack was encrypted, and the attackers were unlikely to have been able to read it.

However, the FDPIC noted that certain aspects of the data processing agreement between the FSO and Concevis needed to be more clearly defined. He pointed out that the contracts concluded by the Confederation's administrative units with service providers needed to include a detailed description of the data life cycle from data entry to data destruction. He also highlighted the need to clearly regulate the possibility for the FSO or external service providers to carry out checks and audits. Finally, the FDPIC reminded the FSO and Concevis of the recommendations issued in the Xplain case, which are universally valid (see Section 1.2).

New practice and supervisory activities

The FDPIC's activities relating to data subjects' rights

Any person may request information from a data controller as to whether or not their personal data is being processed. This key instrument of data protection law is designed to guarantee transparency and to enable data subjects to monitor the processing of their personal data. However, in light of the number of complaints received, the FDPIC notes that this instrument is often overlooked by controllers.

The FDPIC received a number of complaints regarding potential breaches of the right of access. In several cases, he found that controllers had left access requests unanswered or had simply referred to the general information in their privacy policy instead of providing the information required by law.

As part of his supervisory activities, the FDPIC intervened with data controllers, urging them to respond to access requests and to take the necessary measures to ensure compliance with the requirements of the FADP with regard to granting the right of access. In one case, he opened a formal investigation.

Right of access (Article 25 FADP)

A key instrument of data protection law, the right of access is designed to enable anyone to obtain information from the controller as to whether or not their personal data is being processed.

With this right comes the obligation of the data controller to provide information. If the data controller has personal data relating to the person requesting the information, they must provide it within 30 days. They must also provide information about the identity of the controller, the purpose of the processing and the retention period of the personal data, as well as available information about the origin of the personal data and, if applicable, the recipients or categories of recipients to whom personal data has been disclosed. An extension of the deadline is possible, provided that the new deadline is announced within 30 days.

The controller is obliged to provide information about the personal data processed as such, so that the data subjects can determine which data about them is being processed, in order to verify its accuracy and the lawfulness of the processing and, if necessary, to have it corrected or deleted.

In certain cases, the controller may, in accordance with Art. 26 FADP, refuse, restrict or defer access to the information in question. They must justify this decision so that the data subject can understand the reason or reasons for the restriction of the right of access and check its lawfulness.

Controllers who provide false or incomplete information (violation of the duty to provide information) will face criminal prosecution.

Duty to provide information

As part of the legislative project regarding the Passenger Name Records Act (draft PNRA), the FDPIC highlighted, among other issues, the authorities' duty to provide information (see also Section 1.6). Accordingly, the dispatch on the draft PNRA states that airlines must inform air passengers in writing that their data will be processed not only for processing their flight but also in accordance with the Passenger Name Records Act. The information can be included in the airlines' general terms and conditions. The duty to provide information in accordance with Article 5 of the draft PNRA is justified even if it is a repetition: Passenger Name Records are processed in two completely different contexts (technical processing of flight bookings vs. implementation of the Passenger Name Records Act) and for different purposes (flight bookings vs. combating crime) under the responsibility of different entities (airlines vs. fedpol). The purpose for which the data is processed must be clearly stated in the information provided (see Article 6 paragraph 3 FADP). Further information to be provided to the data subjects will be included in the implementing provisions of the ordinance to the FADP.

Right to erasure of data

During the year under review, the FDPIC noted that data erasure requests were being complied with by private data processors and by the Federal Administration. Any difficulties encountered in erasing data were due to technical constraints rather than a lack of willingness. This can occur, for example, if a private individual shares a data platform with other providers, and the data subject only wishes to have the data of a single provider deleted. In practice, technical dependencies may arise here.

Supervisory activities and campaigns under the new FADP

The new Federal Act on Data Protection has strengthened the rights of data subjects and given the FDPIC additional duties and powers, which he exercises with the following tools and supervisory activities:

Tools

The following tools are available on the FDPIC's website:

- **Reporting forms:**
  Data subjects and third parties can use these forms to report suspected violations of the FADP.
- **Reporting portals for data controllers:**
  Data controllers can use our reporting portals to report a data breach or to notify us of the appointment of a data protection officer.

Supervisory activities

In accordance with the factsheet on the investigation of breaches of data protection regulations, supervisory activities can be categorised as follows:

- **Formal investigations**
  Investigation carried out in accordance with the federal law on administrative procedure into the processing of personal data where there are sufficient indications that federal data protection regulations may be being violated.
- **Informal preliminary investigations**
  The FDPIC carries out informal preliminary investigations to determine whether or not there are sufficient grounds to open a formal investigation.
- **Low-threshold intervention**
  Low-threshold intervention takes the form of a written invitation to the data controller to voluntarily take swift action to ensure compliance with data protection regulations in the case of straightforward issues.

Awareness-raising campaigns

Before taking ex-officio supervisory action against private data controllers or federal bodies, the FDPIC may either use awareness-raising campaigns to draw their attention to privacy risks and measures to mitigate these or provide detailed information about his supervisory activities.

Guidelines and factsheets

If necessary, details of supervisory activities are provided in the form of guidelines and factsheets. During the year under review, the following additional publications were issued:

- Factsheet on planning and justifying online access to personal data (18 June 2024);
- FDPIC guidelines on data processing using cookies and similar technologies (22 January 2025);
- FDPIC guidelines on reporting data security breaches and informing data subjects in accordance with Article 24 FADP (6 February 2025).

Supervisory activities in figures

In the 2024/2025 reporting year, the EDÖB received over 1000 reports. For statistical information, see Table 9 on page 91.

Campaign to raise awareness about the use of the OASI number

The FDPIC has launched a campaign to raise awareness of the obligations of the federal departments and the Federal Chancellery with regard to the systematic use of the OASI number. The campaign sets out to remind these bodies in particular of their obligation to conduct regular risk analyses.

As part of a proactive approach, the FDPIC has launched an awareness-raising campaign aimed at the federal departments and the Federal Chancellery regarding their use of the OASI number. The campaign sets out to remind them of the legal provisions governing the systematic use of the OASI number for purposes other than social insurance and to verify compliance through spot checks.

The Federal Act on Old-Age and Survivors' Insurance (OASIA) contains special provisions that impose a series of technical and organisational obligations on users. These include two specific obligations in Article 153e. Firstly, the departments and the Federal Chancellery are obliged to conduct regular risk analyses on the databases that they operate themselves, focusing specifically on the risk of unlawful merging of databases; secondly, in view of these risk analyses, the bodies in question are also required to keep a register of the databases in which the OASI number is used systematically.

As the FDPIC's contact points within the meaning of Article 28 of the Data Protection Ordinance (DPO), the data protection officers of all federal departments and the Federal Chancellery received written notification from the FDPIC on 26 September 2024 reminding them of their legal obligations under OASIA. Further details were provided at an interdepartmental meeting on 30 October 2024.

The campaign launch was also announced to the federal data protection officers of all the federal offices, at a briefing session on 26 November 2024.

Obligation to appoint a representative under Article 14 FADP

The FDPIC has asked foreign companies that process large volumes of personal data of persons in Switzerland to designate a representative in Switzerland.

In order to ensure that the law applies to all practices that have an effect in Switzerland, even if they are initiated in another country, Article 14 FADP specifies the cases in which a representative in Switzerland must be appointed. The purpose of this appointment is to ensure that data subjects and the authorities have a contact based in Switzerland and to avoid a situation of decreased protection afforded to Swiss residents simply because the data controller is based abroad.

Accordingly, all private companies that process personal data relating to the offer of goods or services or the monitoring of the behaviour of people in Switzerland are required to appoint a representative based in Switzerland, whether the processing is carried out regularly or on a large scale or poses a high risk to the personality of the data subjects.

The FDPIC therefore intervened in a targeted manner at a number of international companies that met the legal criteria in order to verify the appointment of a representative and the publication of their contact details.

On his website, the FDPIC provides comprehensive information on the obligation to appoint a representative under Article 14 FADP (see Data protection/Basic knowledge).

Data security breach reports

The FDPIC has published guidelines on dealing with data security breaches and has opened two investigations into data controllers who failed to inform data subjects of such breaches.

Under the revised Federal Act on Data Protection, data controllers are required to report to the FDPIC any data security breach that is likely to pose a high risk to the privacy or fundamental rights of data subjects. During the year under review, the FDPIC received 363 reports from data controllers under Article 24 paragraph 1 FADP.

Under both the old and the current FADP, data controllers can report data breaches even if they do not anticipate a high risk for the data subjects. These are voluntary reports and are sometimes submitted either because the breaches could spark media coverage or because data subjects or whistleblowers could report them to the FDPIC.

In cases of mandatory reporting, the FDPIC conducts summary checks to determine whether or not the action already taken and further measures planned by the controller are sufficient to protect the data subjects and to minimise damage. If necessary, the FDPIC requests more information

or demands that additional safeguards be implemented in order to protect the data subjects. He also checks whether the data subjects have been adequately informed about the incident. In cases of voluntary reporting, i. e. where the controller has not identified a high risk for the data subjects, he only assesses whether or not there is an obligation to inform the data subjects and, if so, how this obligation was fulfilled.

During the year under review, the FDPIC noted some uncertainty among data controllers regarding the concept of 'high risk', which entails an obligation to notify the FDPIC, and the difference between this and the 'need for protection', which requires the data subjects to be notified. Furthermore, some data controllers appeared unclear about the tasks that they were required to fulfil with regard to receipt and assessment of mandatory and voluntary reports and fulfilment of their obligation to inform the data subjects.

In order to support data controllers in fulfilling their duties and to clarify their role, the FDPIC published guidelines on how to deal with data security breaches on 22 January 2025. In the guidelines, he sets out the criteria that controllers should use to assess whether there is an obligation to notify the FDPIC. He also explains that the data subjects are to be informed if they can or need to take action themselves in order to minimise or avoid damages resulting from a data breach. Such action might include changing login details or passwords, blocking credit cards, double-checking account statements or critically examining all messages and requests (phishing emails).

The FDPIC may demand that the data subjects be informed if he deems that they are in need of protection or if there is a public interest in the controller informing them due to the large number of data subjects affected or media coverage. The FDPIC has the authority to do so regardless of whether the controller reported the breach to him through voluntary or mandatory reporting or whether or not the breach was reported at all.

The FDPIC has opened an investigation under Article 49 ff. FADP into two controllers who either failed to inform the data subjects of a breach or failed to do so adequately where this seemed necessary for their protection. Both controllers believed that they were under no obligation to notify the data subjects and refused to inform them of the breach even after the FDPIC demanded that they do so. The investigations are still ongoing.

Data breaches in figures

In the 2024/2025 reporting year, 363 data security breaches were reported to the FDPIC. The exact figures for the data-breach reports can be found in chapter 3.1.

Increase in the number of DPIA reviews

After the revised Federal Act on Data Protection came into force, the FDPIC received a number of data protection impact assessments (DPIAs) from federal bodies requesting his opinion. A DPIA must be carried out if the processing of personal data is likely to pose a high risk to the privacy or fundamental rights of the data subjects.

The data protection impact assessment (DPIA) is a tool used by data controllers to identify, assess, and mitigate the risks associated with personal data processing. If the DPIA shows that the planned processing still poses a high risk to the privacy or fundamental rights of data subjects despite the measures envisaged by the controller, the FDPIC needs to be consulted.

An exception is made for private data controllers who have consulted their company data protection officer. The FDPIC published a DPIA factsheet with guidance for them in 2023. Most of the feedback from private individuals on use of the tool has been positive, and some have created templates and automated assessment tools. The FDPIC welcomes these private initiatives, especially as they can facilitate the necessary changes to the DPIA.

DPIAs in federal projects

As expected, we received DPIAs from a number of federal bodies requesting our opinion as the relevant Federal Council guidelines require these to be included in the office consultations on draft legislation (e. g. in the consultation on the Passenger Name Records Act (PNRA), see Section 1.6).

In particular, the FDPIC amended the assessments to include a plain-language summary of the risks associated with the envisaged data processing and the measures taken to mitigate them in order to enable the Federal Council and Parliament to make their decisions in full knowledge of the residual risks.

Obligation to log processing activities

The new Federal Act on Data Protection (FADP) and the associated Data Protection Ordinance (DPO) that came into force on 1 September 2023 introduced an obligation to keep records of processing activities in accordance with Article 4 DPO. This means that controllers and their processors are required to keep logs of processes such as storage, alteration, reading, disclosure, deletion and destruction of data for all automated processing of personal data. Log data is used to detect, trace and investigate data breaches.

The obligation to log all processing activities applies throughout the Federal Administration with its large number of applications and has already been in place for more than twenty years for the processing of sensitive personal data and personality profiles. It is also part of the basic ICT protection (numbers T2.1 c and 5) to be implemented by all federal administrative units. Logging is also common practice in the processing of ordinary personal data within the large information systems operated by the Federal Administration such as the electronic records and process management system (GEVER).

Transitional provisions for the introduction of read logging

Article 46 DPO contains a transitional provision designed to align the introduction of read logging as required by Article 4(2) DPO with the development cycles of the ICT systems. Under this provision, for systems that do not fall within the scope of the Schengen Directive (EU) 2016/680, the obligation to log processing activities starts to apply three years after the DPO comes into force (i. e. from 1 September 2026) or at the end of the life cycle of the system in question. This means that the obligation can be deferred until system-related adjustments are needed anyway. This provision is intended to ease the workload so that not all federal information systems need to be modified at once by 1 September 2026.

Challenges and measures

The obligation to keep records applies to data controllers and their processors, who are required to log processes such as storage, alteration, reading, disclosure, deletion and destruction of data for all automated processing of personal data. Logging creates transparency in data processing and enables a swift response in the event of a data breach. Log data is used to detect, trace and analyse data breaches.

However, the obligation to log data can entail considerable additional work and costs for application operators with particular regard to the gradual alignment and scaling of the existing IT infrastructure to meet the new requirements.

The Federal Office of Information Technology, Systems and Telecommunication (FOITT) has drawn up a cost estimate based on experience, which, among other things, has led to calls for risk-based restrictions on the logging obligation as part of the office consultation on the DPO. In 2025, the FDPIC is due to hold roundtable talks with the federal agencies involved in order to take due account of these demands in compliance with the legal requirements.


← 2

1.2 Justice, Police, Security

CYBERCRIME

Investigations into Xplain, fedpol and FOCBS complete: recommendations adopted

The FDPIC discovered violations of data protection law during the course of three investigations into the federal offices of fedpol and FOCBS and the company Xplain. The published results of the investigations showed that personal data had been transferred from fedpol and FOCBS to the private company Xplain without the necessary data protection safeguards in place and had subsequently been stored by Xplain in breach of data protection law and, in some cases, in breach of contract.

In his reports, the FDPIC concludes that neither the Federal Office of Police (fedpol) nor the Federal Office for Customs and Border Security (FOCBS) had established a clear agreement with the private company Xplain as to whether or not and, if so, under which conditions personal data from the federal offices in question could be stored on Xplain's server as part of support services. An express agreement should have been drawn up on the extent to which personal data could be disclosed to and stored by Xplain. The process in place involved the transfer of personal data to Xplain as part of support services without any specific requirements being set for transfer or for the implementation of data security safeguards at Xplain. This resulted in a collection of unstructured data from the federal offices in question on the company's server. The FDPIC also found the amount of personal data transferred as part of the process to be disproportionately large.

Recommendations for outsourcing processing

The Federal Administration is working together with private companies in the operation and development of its digital applications. This collaboration involves outsourcing the processing of personal data. The supervisory investigation into the ransomware incident at Xplain illustrates the high risks and damage potential damage associated with such data transfers. The parties in question have adopted the recommendations, and, from now on, the Federal Administration and all its private data processors are obliged to identify any high risks and take appropriate measures to reduce them to an acceptable level in good time.

Following the findings of the three investigations, they are required to comply with the following key provisions of federal data protection law:

- As 'data controllers' under data protection law, when working with private companies (as 'data processors', for example for the provision of support services), federal bodies must assess whether or not it is necessary for personal data to leave the Federal Administration's protected ICT infrastructure or for contracted private parties to gain access to the infrastructure. They also need to determine whether or not personal data can be anonymised before being sent and what additional technical and/or organisational safeguards are to be implemented in order to prevent data breaches.
- After analysing the data security risks and identifying suitable safeguards to minimise them, the federal bodies and private companies must document their implementation processes, including data flows, anonymisation and access policies, in a clear and exhaustive manner. Federal bodies must also set out the necessary technical and organisational safeguards in contracts concluded with private companies, which, where applicable, should include contractual penalties.
- When processing personal data, private data processors are required to observe the contractual obligations and requirements in terms of scope, scale and duration. Appropriate measures to ensure compliance with these requirements include policies for the timely deletion of data, training employees and raising their awareness, and periodic internal or external audits.

Fedpol, FOCBS and Xplain adopted all of the FDPIC's recommendations in connection with the ransomware incident at Xplain by the end of May 2024.

The investigations into the FOCBS and fedpol regarding the legality of access by FOCBS employees to the RIPOL search system operated by fedpol have been separated from the proceedings concerning Xplain and are ongoing.

Checks within the Federal Administration

In his press release of 4 June 2024 issued upon completion of the investigation into the Xplain case, the FDPIC called on the Federal Administration and its private data processors to review their cooperation regarding the processing of personal data based on the findings of the three investigations conducted. In the same statement, we announced checks throughout the Administration.

In September 2024, the FDPIC carried out the first spot checks in the Federal Administration.

LEGISLATION

Revision of the Intelligence Service Act

The Federal Act on the Intelligence Service (IntelSA) is to be revised to redefine and extend the processing of intelligence data.

The Federal Department of Defence, Civil Protection and Sport (DDPS) has divided the ongoing work on revision of the IntelSA into two parts following the administrative investigation into information gathering by the Cyber Division of the Federal Intelligence

Police Enquiry Platform POLAP

The FDPIC's criticism expressed on several occasions throughout the 2023/24 reporting year regarding the plans to link the cantonal police systems at national level via a POLAP enquiry platform operated with the federal government's participation (see also 31st Annual Report, Section 1.2) was acknowledged by the Federal Supreme Court in its decision 1C_63/2023 of 17 October 2024. In the above-mentioned decision, in response to a complaint, the Federal Supreme Court was called upon to rule on a provision of the Canton of Lucerne that sought to allow the cantonal systems to be connected to the POLAP platform as soon as the latter went live. The Federal Supreme Court annulled the provision in question on the grounds that there was no sufficiently clear legal basis for the planned access and that the extensive access provided by search tools violated the principle of proportionality and the rights of data subjects in connection with the administrative assistance procedure.

The revision of the CCJPD's draft agreement on the exchange of police information with the participation of the federal government, recommended by the federal and cantonal data protection authorities, has not yet taken place. The explicit legal basis announced by fedpol for operation of the enquiry platform as part of Switzerland's national strategy for combating organised crime is also pending. The FDPIC expects the Confederation and the cantons to continue their work in the upcoming reporting period, to keep him and his cantonal counterparts updated on further action, and to consult them in good time on all data protection-related issues.

Service (FIS). The FDPIC has already commented on the first part and on the amendment of the right to information regulated therein (see 29th Annual Report, Section 1.2).

The revision provides, among other things, for a redesign of intelligence data processing, whereby the bill specifies the categories of personal data processed instead of individual information systems. A complementary consultation procedure on the second part of the revision is set to take place by July 2025. The FDPIC is accompanying the work.

1.3 Economy and society

CROSS-PLATFORM TRACKING

Ricardo and TX Group's response to the final report and recommendations

During the year under review, the FDPIC published his final report after giving Ricardo and the TX Group an opportunity to comment on his recommendations. The FDPIC assesses further action after his conclusions were rejected.

In spring 2024, the FDPIC closed the proceedings that he had opened against Ricardo and the TX Group (TX) under the old law concerning the Ricardo auction platform and cross-platform tracking for targeted advertising purposes.

In his final report, the FDPIC recommended, in particular, that Ricardo modify its platform so that users are informed in a clear and transparent manner of the tracking carried out by TX and the purposes pursued and that it obtain users' consent before sharing their data with TX for targeted advertising purposes. It recommended that TX delete the data already shared in this context as the company lacked the necessary consent (see 31st Annual Report, Section 1.3).

Both companies commented on the FDPIC's final report and recommendations. In their respective statements, Ricardo and TX argued that the data shared did not constitute personal data and that the Federal Act on Data Protection therefore did not apply. The companies stated that they would not be following the recommendations, which they considered legally unfounded or not applicable, arguing that they related to a situation that no longer existed and legislation that was no longer in force.

The FDPIC reserved the right to take appropriate measures to have the required changes to the Ricardo platform implemented if the breaches

Guidelines on data processing using cookies and similar technologies

The use of cookies and similar technologies by website and app operators and the associated processing of personal data affects everyone who uses the internet on a daily basis. The FDPIC analysed these types of data processing in detail in his investigations into the Ricardo auction platform and Digitec Galaxus in applying the previous version of the FADP. The revised Federal Act on Data Protection – which introduces changes such as replacement of the concept of 'personality profile' by the concepts of 'profiling' and 'high-risk profiling' – prompts the question as to what new aspects website and app operators need to consider when using cookies and similar technologies.

On 22 January 2025, the FDPIC published a set of guidelines to shed light on this topic and to clarify his supervisory activities under the new law. The guidelines are aimed primarily at private data controllers but also include references to the special provisions applicable to federal bodies.

The guidelines explain the following:

- that the special provision in Article 45c of the Telecommunications Act is to be applied in conjunction with the general requirements of the FADP;
- the responsibilities of website operators when using third-party services and third-party cookies;
- how they can fulfil their duty to provide information in this context; and
- how they can grant data subjects their right to influence a legal relationship and implement it in a legally compliant manner in such a way as to validly obtain justifiable consent and implement the legal right to object.

identified in his final report persisted. On 22 January 2025, he published guidelines on the use of cookies containing specific guidance on the requirements that need to be met in order to ensure compliance with the new FADP.

At the request of Ricardo and TX, the PFPDT published a redacted version of its final report in October 2024, accompanied by a press release. Following an access request granted under the Freedom of Information Act (FoIA), the unredacted report was published on the PFPDT website in March 2025.

CUSTOMER ACCOUNT

FDPIC monitors implementation of recommendations adopted by the online shop

On 15 April 2024, the FDPIC concluded his investigation into Swiss online retailer Digitec Galaxus and issued formal recommendations. He is currently overseeing implementation of the recommendation adopted by the retailer, which is scheduled for the second quarter of 2025.

The recommendation adopted by the Swiss online platform Digitec Galaxus concerned its failure to provide users with the option to object to the data processing under investigation, which the company carries out primarily for marketing purposes. Users are required to create a customer account before they can place an order. However, since the data processing involved is not strictly necessary for the conclusion of a sales agreement, linking this data processing with the customer account violates the principle of proportionality (see 31st Annual Report, Section 1.3). Therefore, the FDPIC recommended that Digitec Galaxus amend its data processing activities to ensure that they did not encroach more than necessary on customers' right to informational self-determination.

In December 2024, Digitec Galaxus presented the FDPIC with a possible solution for implementing the adopted recommendations, which the FDPIC had formulated under the old FADP. Digitec Galaxus informed us that the recommendations would be implemented in the second quarter of 2025. On 22 January 2025, the FDPIC published comprehensive guidelines on the use of cookies containing specific guidance that Digitec Galaxus needs to follow in order to ensure compliance with the data protection requirements of the new FADP.

ONLINE CAMPAIGN

Investigation into the association 'Bürgerforum Schweiz'

The FDPIC has investigated the data processing activities of the Swiss citizens' association 'Bürgerforum Schweiz' in connection with its online campaign to gauge priests' core beliefs. As part of the campaign, the association collects the contact details of priests and other people working in the church environment in order to send them a questionnaire. Recipients of the questionnaire and their responses are published in an online database along with other information. As some individuals are listed in the database against their will, the FDPIC ordered an administrative measure on which the Federal Administrative Court must now rule.

The FDPIC became aware of the data processing activities of the citizens' association in connection with its online campaign to gauge priests' core beliefs back in 2023. The association collects the personal details of people working in the church environment (priests, church council and synod members, university employees, youth workers etc.) whose addresses are publicly available in order to send them a questionnaire. The purpose of the questionnaire is to establish whether the individuals in question share the association's core beliefs. The association manages a publicly accessible database containing this information and had refused to delete entries regarding persons who were listed in the database against their will at their request (see 31st Annual Report, Section 1.3).

At the end of 2023, the FDPIC launched a formal investigation into the data processing activities in question in order to assess compliance with data protection law. He concluded, among other things, that the association was violating the principle of proportionality by including in the publicly accessible database the details of individuals who had only been 'recorded' or merely 'asked'. In the FDPIC's view, this data is neither appropriate for obtaining reliable information about the beliefs of the persons concerned, nor is it necessary for the purpose of producing a representative survey. Publication of such data therefore requires justification under data protection law.

In the FDPIC's view, there is no overriding private or public interest that would justify labelling persons who are publicly recorded elsewhere with the status of 'recorded' or 'asked' in the database. Therefore, individuals may be recorded in the database – regardless of whether or not their details are published elsewhere – only with their legally valid prior consent. If an individual has already submitted a deletion request, their data must be deleted. The FDPIC ordered an administrative measure to that effect in spring 2024 (see 31st Annual Report, Section 1.3). The citizens' association lodged an appeal against the measure with the Federal Administrative Court in the year under review, and the court's decision is still pending.


Kamera auf den QR-Code richten
Kundenkarten hinzufügen
Cumulus, Supercard und mehr
Kein QR-Code? – Code eingeben
0.85
Stop
OK

THE HOUSING MARKET

Unacceptable questions on tenancy application forms

Tenancy application forms provided by landlords are required to comply with data protection law. The FDPIC clarifies the legal situation under the new FADP and warns property management companies that use information-gathering forms that encroach on applicants' privacy.

The FDPIC had already issued recommendations back in the 1990s on the handling of applicants' personal details in connection with rental properties (see 4th Annual Report 1996/1997, p. 49). Obtaining data on prospective tenants is generally permitted as long as such information is relevant for the purpose of selecting a suitable tenant on the basis of objective criteria. In particular, data processing must be carried out transparently and for a specific purpose. In this case, the purpose is defined as the prospective signing of an agreement. In accordance with the principle of proportionality, only data that is objectively necessary in order to accomplish said purpose may be obtained and processed. Data processing must not unnecessarily infringe upon the privacy of data subjects. A 1996 decision by the former Data Protection Commission largely confirmed the FDPIC's view and forms the cornerstone of his long-standing practice.

During the year under review, the FDPIC had a chance to address this issue again and to review his practice following the revision of the Federal Act on Data Protection based on specific examples. He received numerous complaints from data subjects regarding application forms, and the media also repeatedly drew the FDPIC's attention to questionable examples. The FDPIC therefore conducted a campaign in the year under review that included measures on three levels:

In particular, as part of his awareness-raising mandate, he revised the fact-sheet for tenancy application forms in order to clarify the data protection requirements. He simplified the wording and included examples that illustrate how landlords can obtain and process the details of prospective tenants in compliance with the principles of the FADP.

In his advisory role, the FDPIC engaged in dialogue with the Swiss Real Estate Association (SVIT) and the Swiss Homeowners' Association (HEV). We reiterated our position regarding the unacceptability of asking about marital status, nationality, place of origin, religion and current living situation and requesting copies of ID. However, the industry's arguments convinced us that a copy of the extract

from the debt enforcement register can reasonably be requested from all applicants as part of the application process, and not just from the chosen tenant, as the FDPIC had previously argued. However, it is important that these copies are destroyed immediately for prospective tenants that are turned down. The factsheet has been amended accordingly. The FDPIC also shared the revised factsheet with the Tenants' Association.

The FDPIC took the opportunity to draw the industry's attention to further data protection issues in the context of the rental process such as the disclosure of information about the current tenant for the purpose of arranging a viewing of an apartment and taking photographs of the occupied apartment without the tenant's consent. Following the exchange, the SVIT included these points in its industry recommendation regarding the collection of personal details in tenancy application forms.

As part of his supervisory activities, the FDPIC reviewed the application forms of various property management companies in the German- and French-speaking parts of Switzerland that had been reported to him. Where information was requested in violation of the principle of proportionality, he contacted the data controllers in writing (low-threshold intervention). In particular, the forms requested information about nationality, marital status and the existence of a guardianship. Unacceptable questions were also asked about the prospective tenants' previous living situation, for example the duration of the tenancy agreement, the number of rooms or the amount of rent paid. Some property management companies also systematically requested pay slips for the previous three months or original extracts from the debt enforcement register, or their forms contained a blanket declaration of consent that allowed the landlord to obtain all other necessary information about the applicant. In one case, the property manager had gone as far as employing a private investigator to carry out enquiries about an applicant with third parties.

Although the FDPIC's interventions were largely successful, not all of the property management companies contacted were willing to review their practices voluntarily. Therefore, the processing of personal data for the conclusion of rental agreements is likely to continue to occupy the FDPIC in the coming year due to increasing digitalisation in the real-estate sector.

1.4 Health

DOPING

Transmission of Swiss athletes' medical information

The systematic transmission of medical records to the World Anti-Doping Agency (WADA) for spot checks is considered disproportionate and lacking a sufficiently specific legal basis. WADA had asked Swiss Sport Integrity (SSI) to implement this measure. However, following the intervention of the FDPIC, SSI will be able to continue its current practice.

In the fight against doping, Swiss Sport Integrity works together with WADA, whose job it is to ensure compliance with the World Anti-Doping Programme. WADA conducted an audit at SSI and ordered a number of measures. One of these measures concerned the data of athletes with a Therapeutic Use Exemption (TUE), i. e. special permission to use a doping substance to treat a medical condition. WADA requested that the ISS systematically submit the medical records of all athletes with a TUE for the purpose of spot checks. Up until then, SSI had only ever sent a brief summary of an athlete's state of health, and their medical record was only sent if WADA wished to test a specific athlete. This new practice would have involved far more extensive data processing, and so SSI contacted the FDPIC.

In a letter that SSI then sent to the WADA, the FDPIC pointed out that any processing of personal data had to comply with the principle of proportionality. After reviewing the case, he concluded that the change requested by WADA was not proportionate: The systematic transmission of the medical records of all athletes with a TUE was not necessary for WADA's monitoring activities, which were limited to spot checks. The current practice is effective and allows WADA to carry out tests whenever it wishes, so the change requested does not meet a real need. At the same time, athletes are keen to ensure that their sensitive data is only transmitted if a test is actually carried out. In this regard, the FDPIC also pointed out that sending data to a third party posed an additional risk, particularly when the latter was located abroad (WADA is based in Canada). Such a risk therefore had to be justified by an overriding interest, which was not present in this case.

The FDPIC also pointed out that, in all likelihood, SSI lacked a sufficiently specific legal basis that would allow the systematic transmission of data as requested.

WADA took the FDPIC's opinion on board and accepted that SSI continue with its current practice. The matter is now closed.

PATIENT CONSENT FORMS

Duty to provide information and obtaining consent

The consent form handed out to patients when they visit a doctor or other healthcare professional raises a number of questions. Given the confusion that patients sometimes experience with this form, which includes a number of legal aspects, the FDPIC intends to raise awareness among service providers and their governing bodies of the FADP requirements in this regard.

During the year under review, the FDPIC was contacted on a regular basis and asked for his views on aspects relating to patient consent forms. He will shortly be publishing information on his website for service providers and their governing bodies explaining how they need to modify their forms in order to meet the requirements of the Federal Act on Data Protection (FADP).

Broadly speaking, in terms of data protection, it is important to distinguish between the requirements relating to the obligation to provide information and those relating to consent.

Duty to provide information

For doctors and other healthcare professionals, the duty to provide information is nothing new as it already existed under the old FADP for processing that involved sensitive data such as health information. Under the new FADP, the duty to provide information is extended to all categories of personal data.

The information to be provided includes all the details needed in order to guarantee transparency of processing and to enable the data subject to assert their rights. The information must be adapted to the situation at hand and must include at least the data referred to in Article 19 paragraph 1 FADP. The degree of detail will depend on the type of data collected, the nature and extent of the processing, the risk of a data breach, and the seriousness of a breach of personality rights.

There are no specific requirements as to the form in which the information is to be provided. The information must be transparent, clear, concise and easily accessible. Although the information may be provided verbally, it can be useful to use the written form and document the provision of information in order to secure proof of compliance with the duty to provide information. However, the patient is free to decide whether or not to read the document and is not obliged to acknowledge receipt or confirm their consent. In practice, it is sufficient to provide information in a form or to hand out an information sheet, which the patient may be asked to sign to acknowledge receipt.

Consent

Here too, there are no major changes in the new FADP. Consent is not, in principle, a prerequisite for data processing but is taken into consideration as justification, particularly when sensitive personal data is shared with third parties. In other cases, processing may be justified by an overriding private interest when the processing is directly related to the conclusion or performance of a contract.

For consent to be valid, it must be informed and given freely before or at the start of the data processing for which it is required, and the data subject must receive at least the information specified in Article 19 FADP. Depending on the context and the nature of the data being processed, it may be necessary to provide more detailed information that will enable the data subject to assess the scope of the authorisation; this means that consent must be given for one or more specific instances of data processing and must include all the purposes of processing; it cannot be given generally for all future processing.

There are no specific requirements as to the form in which consent is given. Therefore, it does not need to be given in writing. However, the data controller is required to provide proof of consent. It is therefore in the controller's interest to document the receipt of consent.

ELECTRONIC PATIENT RECORD

Full revision of the Act and transitional funding

The electronic patient record (EPR) is being developed on an ongoing basis. The proposal for a comprehensive revision of the Act submitted for consultation advocates greater centralisation. On this basis, the Federal Council has decided that in future it will be up to the Confederation to provide and develop the required technical infrastructure. Meanwhile, Parliament has approved transitional funding to support the use and development of the EPR. The FDPIC is monitoring the progress of the work.

In summer 2023, the Federal Council submitted for consultation a proposal for a comprehensive revision of the Federal Act on the Electronic Patient Record, which the FDPIC had commented on (see 31st Annual Report 2023/24, Section 1.4). The revision included a number of measures designed to further improve and develop the electronic patient record, for example making it compulsory for all service providers to register and introducing an opt-out model (right to object instead of explicit consent). In addition, the revision regulates the roles of the Confederation and the cantons more clearly with regard to the EPR.

In view of the critical feedback regarding the decentralised structure of the EPR, the Federal Council is now planning to centralise the EPR to a greater extent. On this basis, at its session on 27 September 2024, it decided that in future it will be up to the Confederation to provide and develop the required technical infrastructure. Up until now, the entire EPR technical infrastructure has been provided by the communities and reference communities, which use different IT platform providers.

The dispatch on the comprehensive revision includes this amendment and is expected to be submitted to Parliament in autumn 2025.

Transitional funding, consent and access to data search services

As the comprehensive revision of the Act required for development of the electronic patient record is expected to take several years, the Federal Council has submitted to Parliament, as part of a separate revision of the EPR Act, a plan for transitional funding for EPR providers (reference communities) to encourage the immediate roll-out and use of the EPR. In order to support the use and development of the EPR, in spring 2024 Parliament approved financial aid amounting to CHF 30 for each EPR opened, to be paid for five years from the entry into force of the above-mentioned amendment to the Act. This transitional funding came into force on 1 October 2024.

The partial revision will also make it possible to register the EPR as an instrument of the compulsory health insurance system which will simplify the process of opening records. Patients are now able to consent to the opening of an EPR using an electronic means of identification issued by a certified issuer, meaning that a handwritten or digital signature is no longer required. In addition, the cantons will have access to the data search service of healthcare institutions and healthcare professionals in order to check compliance with the obligation for hospitals, birthing centres, nursing homes and physicians admitted after 1 January 2022 to join a certified community or a reference community.

The FDPIC will continue to actively monitor the development of the EPR and ensure that data protection requirements are met, particularly during consultations with the authorities on its implementation and in relation to specific issues.

1.5 Employment

FEDERAL PERSONNEL LAW

Whistleblowing platform

The FDPIC has advocated on a number of occasions that the processing of data relating to whistleblowing reports submitted by federal administration employees should be regulated more precisely in law.

As part of the draft revision of the Federal Personnel Act (FPA), the FDPIC has called for improvements to the provisions regulating the processing of data carried out in connection with whistleblowing reports. Federal administration employees are obliged to report all crimes and offences that are prosecuted ex officio which they have come across or which have been brought to their attention in the course of their work. They are required to report them to their superiors, to the Swiss Federal Audit Office (SFAO) or to the criminal prosecution authorities. They may also report other irregularities that they have discovered or which have come to their attention in the course of their work.

However, Article 22a FPA, which provides for reporting to the SFAO's whistleblowing platform, is currently incomplete. While the SFAO's legal duties are set out in the FPA, and the whistleblowing register has been duly declared to the FDPIC, data processing as such is not defined in the Act. The article merely states the following: «The SFAO clarifies the facts and takes the necessary measures». The processing of sensitive personal data by the SFAO needs to be regulated in detail in law. This is especially important as whistleblowing reports may mention names, and some may include specific individuals and sensitive data, as for example in cases of indiscretion or offences under criminal law (corruption, embezzlement, irregularities in public procurement etc.).

The views expressed by the FDPIC in the office consultation procedures were taken on board, and changes have been made to the draft revisions of three different pieces of federal legislation. These changes concern the clarification required regarding whistleblowing reports themselves, whistleblowing procedures, and the processing of the associated data.

The draft revision of Article 22a FPA has been amended to clarify the reporting conditions and the bodies to which whistleblowing reports may be submitted. In particular, the Act now clearly regulates the option for employees of the Federal Department of Foreign Affairs (FDFA) to submit reports directly via the FDFA whistleblowing platform.

In addition, a new article (Article 10a) has been introduced in the Federal Audit Office Act (FAOA; SR 614.0) containing provisions specific to the data processing carried out by the SFAO in connection with whistleblowing reports. These draft provisions govern, among other things, operation of the reporting office, the processing of sensitive data carried out by the latter, and the sharing of data with other authorities. Finally, the processing of data from reports submitted via the FDFA platform has been regulated in the Federal Act on the Processing of Personal Data by

the Federal Department of Foreign Affairs (SR 235.2). A new Section 10 'Persons involved in reporting crimes, offences and irregularities' has been introduced in the draft in order to regulate the data processing activities that will be carried out by the FDFA in connection with reports falling within the scope of Article 22a FPA that will be submitted via its whistleblowing platform.

Developed based on the FDPIC's input and introduced as part of the revision of federal legislation, these amendments are intended to provide legal certainty with regard to the processing of data in connection with whistleblowing reports and to provide a sufficiently detailed legal framework.

FEDERAL PERSONNEL LAW

Profiling as part of assessments and active recruitment

In connection with the revision of the Federal Personnel Act, the FDPIC issued a number of statements calling for a sufficiently precise and transparent legal basis for profiling conducted as part of assessments and active recruitment. He also demanded that data protection impact assessments be carried out prior to such data processing activities taking place in order to assess the associated risks and define appropriate safeguards.

In connection with the revision of the Federal Personnel Act (FPA), the FDPIC commented on various aspects of data protection. In the revised FADP, the term 'personality profile' has been dropped, and the terms 'profiling' and 'high-risk profiling' have been introduced. Therefore, the FPA needs to be updated to reflect the new terminology, with particular regard to assessments (evaluations and personality tests for employees and job applicants) and active recruitment. While assessments are already provided for in the current FPA, the active recruitment process, i. e. the processing of data on individuals who are neither job applicants nor employees, has yet to be enshrined in law.

The provisions of the FPA needed to be amended in line with the new term of profiling so that the federal government as an employer could continue using assessments in staff recruitment, promotion and development in the future, for example to assess whether or not an employee was suitable for a given project or for a promotion, or to recommend a career path to them.

In addition, a legal basis is needed for active recruitment to allow employers to use social media (for example LinkedIn) to search for suitable candidates and to assess a person's suitability for a specific post.

Depending on the circumstances, this type of data processing can constitute not only profiling but high-risk

profiling as even information that is harmless on its own can easily be aggregated to create a comprehensive profile of a person, revealing significant aspects of their personality. Therefore, a sufficiently clear and detailed legal basis is required in order to ensure compliance with the principles of legality and transparency. In particular, categories of sensitive data need to be defined and enshrined in law for the various operations. In response to the FDPIC's comments, the Federal Office of Personnel (FOPER) has amended and clarified the provisions accordingly.

The FDPIC also argued that data protection impact assessments needed to be carried out for the processing activities envisaged in the revised act on account of the high risk that profiling can pose to the privacy of data subjects due to the nature and scope of the processing. The associated risks must therefore be identified and appropriate safeguards defined in order to mitigate the risks. The FOPER then carried out the required risk assessments, during which it identified the associated risks and defined the appropriate safeguards to mitigate them: The latter include a legal framework for access rights, data security measures, employee training and awareness-raising, the introduction of instructions, and the logging of data processing activities. The results of the risk assessments were presented in the Federal Council's dispatch to Parliament.

EMPLOYEE MONITORING

Compliance with data protection principles in employee monitoring

The use of surveillance in the workplace has prompted several interventions by the FDPIC. In order to ensure compliance with data protection regulations, data processing must be limited to what is strictly necessary, and employees must be adequately informed in advance.

During the year under review, the FDPIC received an increased number of enquiries regarding the privacy compliance of video surveillance systems. In some cases, he took action in the form of preliminary enquiries and low-threshold intervention, drawing attention to the principles of data protection. He also opened an investigation into one surveillance system.

An employer may only process data concerning an employee if it relates to the individual's suitability for the job or is necessary for the performance of


65797 km
PARK
D / B
N
R

the employment contract (principle of proportionality). However, the employer has a duty to protect the health and privacy of employees. Therefore, the use of surveillance systems specifically to monitor employee behaviour is prohibited. If surveillance is required for any other reason, it should be set up in such a way as not to affect employees' health and freedom of movement and must be limited to what is necessary. In the case of a video surveillance system, this means, for example, that the recordings may not be used to monitor the behaviour of employees and that the employer must have a legitimate business interest that outweighs the interests of employees with regard to the protection of their privacy. The video cameras must be positioned and set up in such a way that the recording area is kept to a minimum and employees have areas of privacy. Filming in break areas is generally not permitted.

Transparency is also important. Employees must be fully and clearly informed about the type, purpose and scope of a surveillance system before it is used. In practice, shortcomings are often observed in this respect: employees are often not or not sufficiently informed about the use of surveillance systems.

Compliance with these principles is crucial as the validity of consent in relation to surveillance systems is limited in the workplace given that an employee's freedom to decide is restricted by their being in a subordinate relationship with their employer.

Employee monitoring

Employee monitoring is a topic that the FDPIC deals with again and again: digital time recording, GPS tracking and access to employees' work emails are just a few examples of areas that often raise privacy issues. The investigation into digital time recording at a building cleaning firm is now complete (see 27th Annual Report, Section 1.6).

1.6 Transport

SWISSCOM BROADCAST PROJECT

The FDPIC demands answers regarding Swisscom's drone network

Swisscom Broadcast's Swiss drone network offers a new infrastructure for providing automated drone flights in the coming years. The infrastructure will offer drones as a service for example for industrial inspections, police deployment and the protection of large-scale sites.

The FDPIC has carried out clarifications into service provider Swisscom Broadcast to ensure that personal data is processed in accordance with data protection regulations when the infrastructure is deployed. He has found that the drone network operator is taking the necessary measures to ensure data protection. These include drawing up a preliminary risk assessment before commissioning the drone network and a data protection impact assessment if there are high risks to the privacy or fundamental rights of data subjects. The FDPIC will continue to monitor the development of this infrastructure and communicate regularly with the operator.

BIOMETRICS

Facial recognition at Zurich Airport

Facial recognition at Zurich Airport should be introduced only if there is a legal basis. The FDPIC has reviewed the project in depth as it carries potentially high risks to the personal and fundamental rights of data subjects.

Flughafen Zürich AG has informed the FDPIC of its plan to introduce automatic facial recognition technology to identify air passengers. The FDPIC was asked for an initial assessment of the project from a data protection perspective. Biometric data would be used for boarding pass control and, ultimately, to identify air passengers. This is classified as sensitive personal data within the meaning of the FADP, and the processing of such data poses a high risk to data subjects' privacy and fundamental rights.

As the holder of an operating licence governed by the Federal Aviation Act, Flughafen Zürich AG is considered a federal body within the meaning of the FADP. The processing of sensitive personal data by federal bodies requires a formal legal basis. The Aviation Act, which is currently being revised, envisages the use of biometric data for checking boarding passes in accordance with international regulations. However, until the revised act comes into force, there is no formal legal basis. Therefore, the use of biometric data is only permitted under the framework conditions applicable to a pilot test in accordance with the FADP.

Flughafen Zürich AG says that it plans to use facial recognition exclusively for boarding pass control and on a voluntary basis. In addition, Zurich Airport will provide clear signage indicating the areas in which passengers can be biometrically identified in future. The FDPIC has analysed the legal and technical data-processing setup in detail and will continue to provide Zurich Airport with supervisory support during the implementation of this project.

PASSENGER NAME RECORDS

Passenger Name Records Act

At present, the systematic use of passenger name records is not permitted in Switzerland as there is no legal basis in place. A legal basis is currently being developed with the Passenger Name Records Act (PNRA). The Federal Council submitted a legislative dispatch to Parliament on 15 May 2024. The National Council and Council of States approved the law on 21 March 2025. The referendum period runs until 10 July 2025.

Air passengers are required to provide airlines and travel agencies with personal details such as their first and last names, contact details (including address and telephone number), and travel agency and payment information when making a booking. Collection of these passenger name records (PNR) is governed by international regulations issued by the UN, the International Civil Aviation Organization (ICAO) and the EU. PNR data is used to combat terrorism and serious crime. The US has made disclosure of PNR data a condition for Switzerland to remain in the Visa Waiver Programme (VWP), which allows visa-free entry to the United States for tourism and/or business purposes (see also the articles on BTLE and EDPB in Section 1.7).

In addition to the draft Passenger Name Records Act (PNRA), the FDPIC has also reviewed the data protection impact assessment prepared by the competent federal office. The clarification that he requested has been included. The FDPIC will continue monitoring the project.

IT PLATFORM NOVA FOR PUBLIC TRANSPORT

Checks at SBB

The FDPIC has reviewed the data protection improvements that he had called for in relation to the central sales platform NOVA for public transport.

Following an issue reported in February 2022 concerning the central sales platform NOVA operated by Swiss Federal Railways (SBB) on behalf of the Swiss public transport industry organisation Alliance SwissPass (ASP) (see 29th Annual Report, Section 1.7, and 31st Annual Report, Section 1.6), the FDPIC requested that SBB carry out an audit in order to determine whether the required deletion rules had been implemented in NOVA.

Furthermore, the industry organisation has set binding information security standards (Regulation 591) effective from 1 January 2024, with which transport companies that use the NOVA platform are required to comply. Transport companies that already used the platform were required to prove that they complied with the requirements in question by carrying out a self-assessment by the end of June 2024 at the latest. Therefore, the FDPIC asked SBB to report on this as well.

SBB informed the FDPIC that it had carried out an audit in early 2024, during which it had ascertained that the deletion rules in question had been fully implemented in all NOVA applications. At the same time, the necessary structures had been created so that Regulation 591 could be audited and developed on an ongoing basis. We will have a more objective picture of the current situation later in 2025. The FDPIC will continue monitoring the project.

1.7 International

Given the presence of global tech companies in the Swiss market, the FDPIC is faced with numerous cross-border enforcement issues. The modernisation of data protection legislation in Switzerland, Europe and worldwide means that there are now better tools for solving these issues.

Cross-border cooperation with foreign data protection authorities is essential for enforcing the FADP and international agreements with companies operating globally. A swifter exchange of information in the provision of international administrative assistance strengthens the legal protection of data subjects and provides greater legal certainty for data controllers.

In informal 'adequacy groups', the FDPIC exchanged views on this topic with the data protection authorities of countries that the EU formally certifies as providing an equivalent level of data protection in terms of data protection legislation and its enforcement. With regard to social media platforms and other services offered by large international companies, we identified opportunities to speed up cross-border administrative assistance and simplify the transmission of documents.

On the one hand, the Council of Europe Convention on the Service Abroad of Documents Relating to Administrative Matters (SR 0.172.030.5 – EÜZ – which also applies to data protection supervisory authorities – simplifies the exchange of documents between the contracting states; On the other, the FADP authorises the FDPIC to declare that Switzerland allows direct transmission of documents to foreign data protection authorities provided the latter reciprocate in favour of the FDPIC.

DATA SCRAPING

Concluding joint statement on data scraping

After issuing a joint statement on data scraping in 2023, the FDPIC and his counterparts from 16 other data protection authorities engaged with some of the world's largest social media companies. The collaboration culminated in the publication of a concluding statement laying out additional takeaways for industry.

The mass collection of personal data from social media platforms, particularly for training artificial intelligence systems, raises growing concerns. Therefore, data protection authorities from around the world have issued a follow-up statement to the 2023 joint statement. The follow-up statement provides additional guidance to help companies ensure that personal information of their users is protected from unlawful scraping. In particular, organisations should:

- Comply with privacy and data protection laws when using personal information, including from their own platforms, to develop artificial intelligence large language models;
- Deploy a combination of safeguarding measures and regularly review and update them to keep pace with advances in scraping techniques and technologies; and

- Ensure that permissible data scraping for commercial or socially beneficial purposes is done lawfully and in accordance with strict contractual terms.

The initial joint statement was signed in 2023 (see 31st Annual Report, Section 1.7) and submitted to the parent companies of YouTube, TikTok, Instagram, Threads, Facebook, LinkedIn, Weibo and X (the platform formerly known as Twitter).

This led to dialogue between data protection authorities and several of these social media companies as well as with the Mitigating Unauthorized Scraping Alliance, an organisation that aims to combat unauthorized data scraping. The exchange enabled data protection authorities to gain a deeper understanding of the challenges that organisations face in protecting against unlawful scraping, including increasingly sophisticated scrapers, ever-evolving advances in scraping technology, and the difficulty in differentiating scrapers from authorised users.

Generally, social media companies indicated to data protection authorities that they have implemented many of the measures that were identified in the initial statement. Some of the additional measures that were presented in the follow-up joint statement include using platform design elements that make it harder to scrape data using automation, safeguards that leverage artificial intelligence, and lower cost solutions that small and medium-sized enterprises could use to meet their safeguarding obligations.

SWISS- US DPF

Framework for data transfers to the US

Following an agreement between the EU and the UK with the United States on a framework for data transfers to the US in 2023 (see 31st Annual Report, Section 1.7), an analogous Data Privacy Framework for transfers between Switzerland and the US (Swiss-US DPF) came into force on 15 September 2024. As a result, the US was added to the list of adequate states to be approved by the Federal Council, whereby the adequacy of the US is limited to US companies certified under this framework. In addition to the DPF, the legal framework on which the Federal Council's adequacy decision is based also includes Executive Order 14086 on the introduction of a two-tier redress mechanism and additional guarantees for data subjects along with various implementing provisions with which the US Department of Justice substantiates the guarantees set out in the order.

The two-tier redress mechanism is intended to improve the legal remedies set out in the Schrems II ruling on the

one hand and to remedy the weaknesses of the former Swiss-US Privacy Shield on the other. Complaints are investigated in the first instance by the US Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (ODNI). Once the CLPO's investigation is complete, the data subject can appeal the decision in a second instance to the newly created Data Protection Review Court (DPRC).

Complaints submitted to the FDPIC

Throughout the entire procedure, communication between the US authorities and the data subject in Switzerland takes place exclusively via the FDPIC. In the first instance, the data subject submits a complaint to the FDPIC, who will then check to ensure that it is complete before submitting it to the CLPO-ODNI. The FDPIC will determine whether or not it meets the requirements of a 'qualifying complaint'. In order to be considered as such, the complaint must be submitted in writing. The complainant must prove their identity and provide the basic information needed in order to review the complaint. The complainant is not required to prove an alleged interference by the US authorities but merely to provide prima facie evidence. The complainant must also state, among other things, the specific means by which their data was transferred to the US. If all the requirements are met, the FDPIC will then forward the complaint to the CLPO-ODNI.

After the CLPO has completed their review, the FDPIC will inform the complainant that the review is complete and that either no violations have been identified or that the CLPO-ODNI has ordered an appropriate remedy. The standard response issued will neither confirm nor deny that the complainant has been the subject of US intelligence activities. The data subject will also receive the same standard response – again via the FDPIC – for complaints appealed to the DPRC. A similar procedure with standard responses is also used in Switzerland in dealing with requests for information under the Swiss Federal Intelligence Service Act.

Non-certified US companies

For data transfers from Switzerland to non-certified US companies, additional guarantees within the meaning of Article 16 paragraph 2 FADP are still required in order to ensure adequate data protection (e.g. standard contractual clauses or binding internal rules on data protection). However, it should be noted that the guarantees and legal recourse options introduced by EO 14086 apply to all data transfers from Switzerland to the US and not just those carried out on the basis of the Federal Council's adequacy decision within the meaning of Article 16 paragraph 1 FADP.

SCHENGEN

Evaluation of Switzerland

A group of European experts visited Switzerland (an associate member of Schengen) between 20 and 24 January 2025 to evaluate the implementation of the Schengen acquis in the field of data protection.

A team comprising experts from the data protection supervisory authorities of the Schengen Member States (peer-to-peer approach), an observer from the European Data Protection Supervisor (EDPS) and a representative of the European Commission visited Switzerland to evaluate the implementation of the Schengen acquis in the field of data protection.

As part of the multiannual evaluation programme for 2023–2029, all Schengen Member States are evaluated on their overall performance in the implementation of the Schengen acquis in relation to the management of external borders, internal borders without border control, visa policy, returns, large-scale IT systems supporting application of the Schengen acquis, police cooperation, judicial cooperation in criminal matters and data protection. The third generation of Schengen evaluations aims to provide a comprehensive picture of implementation of the Schengen acquis in order to reinforce mutual trust in the Schengen area. The evaluation now takes place every seven years instead of every five (see 31st Annual Report, Section 1.7).

The data protection part of the evaluation assesses the effective implementation of the data protection requirements of the Schengen acquis. The FDPIC was actively involved in the work carried out for the Schengen evaluation of Switzerland in this area. He received the European experts at his offices on 20 January 2025 and explained his role and activities to them and answered their questions.

European law stipulates that four weeks after the evaluation has been completed, the European Commission must send the draft evaluation report and the draft recommendations to Switzerland. Switzerland then has two weeks to respond. The evaluation report analyses qualitative, quantitative, operational, administrative and organisational aspects and lists the shortcomings, areas in need of improvement and good practices identified during the evaluation.

SCHENGEN

SIS, VIS and Eurodac Supervision Coordination Groups

The VIS Supervisory Coordination Group has been transformed into the Coordinated Supervision Committee, which is now also responsible for the EES and ETIAS information systems.

The VIS Supervision Coordination Group (VIS SCG) was brought under the scope of the Coordinated Supervision Committee (CSC). The group still consists of the same data protection authorities, including Switzerland. The chair and secretariat have been transferred from the European Data Protection Supervisor (EDPS) to the European Data Protection Board (EDPB). In future, the CSC will also cover the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS).

The EDPB is currently analysing the number of requests for information or for correction or deletion of data processed in the SIS submitted for the first time by Schengen Member States. It will determine the number of cases in which the request was accepted, i. e. access was granted, or the data was corrected or deleted. The report is due to be completed in 2025.

The Entry and Exit System (EES) was set to be introduced on 10 November 2024 but its launch was delayed due to issues with the stability and robustness of the central database on a European level. The information system is now expected to be rolled out in the Schengen Member States and associate Member States in a phased manner by October 2025.

A representative of the FDPIC also took part in the evaluation of Hungary in the area of data protection.

SCHENGEN

Coordination group of the Swiss data protection authorities

The Schengen coordination group of the Swiss federal and cantonal data protection authorities met twice under the chairmanship of the FDPIC with the data protection authority of the Principality of Liechtenstein as an observer. The FDPIC informed his cantonal counterparts of the outcome of meetings held by the European supervision coordination groups to discuss the existing SIS and VIS information systems and provided an update on the current status of work on implementation of the Entry and Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). Visits to the Federal Office of Police (fedpol) and its SIRENE office also took place. In addition, standard text was created for the cantonal websites regarding the SIS and VIS systems, and the guidelines for SIS checks were updated.

SCHENGEN

Activities at national level

The checks at fedpol as the central access point to the Central Visa Information System (C-VIS) and the inspection of the C-VIS log files at the Swiss Border Guard are complete. The FDPIC also inspected the SIS log files at fedpol's Central Weapons Office.

The checks carried out at the Federal Office of Police (fedpol) looked at the data processing activities of the Operations Centre as the central access point to the C-VIS. During the checks, the FDPIC found no unlawful processing of personal data and was able to conclude the inspection without issuing any orders.

While inspecting the log files and the data processing activities at the Swiss Border Guard, the FDPIC discovered one case of unauthorised access to the SIS. He called on the Federal Office for Customs and Border Security (FOCBS) to make adjustments to the authorisation management and to carry out self-monitoring. The FDPIC will monitor the implementation.

He carried out spot checks of the log files at fedpol's Central Weapons Office in order to verify the lawfulness of access by authorised employees. In order to do so, he asked the fedpol's data protection officer to provide the employee access log for a specific period (4–8 September 2024), which he analysed. In his final report of 19 December 2024, the FDPIC reported no cases of unlawful access.

SCHENGEN

BTLE and EDPB

A subgroup of the European Data Protection Board (EDPB), Border Travel and Law Enforcement (BTLE) deals with matters relating to the Schengen acquis and broader issues relating to the Schengen Association Agreement. Switzerland is involved in the work as a Schengen associate country.

This year, the BTLE subgroup completed its work on the guidelines on Article 37 of EU Directive (EU) 2016/680 (Law Enforcement Directive, LED) (see 31st Annual Report, Section 1.7). Article 37 LED sets out the legal requirements (safeguards) for data transfer to a third country outside the EU/EEA. The guidelines on Article 37 LED were approved and adopted by the EDPB in June 2024.

The FDPIC was also involved in the work on implementation of the Passenger Name Record (PNR) Directive (EU) 2016/681 following the PNR judgement (C-817/19) by the Court of Justice of the European Union (CJEU). The judgement concerns the use of Passenger Name Record (PNR) data for the prevention, detection, investigation

and prosecution of terrorist offences and serious crime and establishes important restrictions on the processing of personal data to ensure that the PNR Directive is applied in compliance with the European Convention on Human Rights (ECHR). Among other things, the judgement rules that PNR data may only be used in connection with terrorist offences and serious crime and sets a strict retention period of up to five years for all PNR data (see also the article in Section 1.6).

Work is also underway on the EDPB's guidance on the interplay between the AI Act and EU data protection law (GDPR and LED).

COUNCIL OF EUROPE

Entry into force of Convention 108+ in prospect

The Council of Europe's modernised data protection convention (Convention 108+) is expected to come into force in 2026. The third and final module of the standard contractual clauses regulating the transfer of personal data to third countries was adopted at the plenary meetings of the Consultative Committee of the Council of Europe's data protection convention along with guidelines on the processing of personal data in connection with voting and elections.

The entry into force of the Council of Europe's modernised data protection convention (Convention 108+) has been further delayed but is expected to take place by the end of 2026. As explained in last year's Annual Report, the modernised convention will only come into force after it has been ratified by 38 Member States (see 31st Annual Report, Section 1.7). The Convention is also open to states that are not members of the Council of Europe and therefore also has an impact beyond Europe. At the end of March 2025, 33 states had ratified the Convention, and 13 states had signed it but not yet ratified it. However, the ratification process is well underway in a number of states, and the Convention is expected to come into force by the end of 2026. Under the modernised convention (C108+), the Consultative Committee will be replaced by a Convention Committee, and an evaluation mechanism will be introduced.

The FDPIC attended the two plenary meetings and the two office meetings of the Consultative Committee on Convention 108+. At its plenary meeting in June 2024, the Consultative Committee adopted the third and final module of the standard contractual clauses regulating the transfer of personal data to third countries. Module 3 covers data transfer from processor to processor, whereas Module 1 covers data transfer from controller to controller, and Module 2 from controller to processor. The three modules have been combined into a single document. The FDPIC recognises these standard contractual clauses of the Council of Europe and has published them on his website. The Committee also adopted guidelines on the protection of individuals in the processing of personal data for the purpose of voter registration and authentication.

During the plenary meeting of November 2024, elections took place to renew the members of the Bureau of the Consultative Committee. The representative of the Argentinian data protection authority was elected as the new chair, and the FDPIC representative as first vice-chair.


Video
control
S
M

SPRING CONFERENCE

European Conference of Data Protection Authorities

The European data protection authorities meet annually for a Spring Conference to discuss matters relating to the exercise of their supervisory activities. The 2024 event was hosted by the Latvian data protection authority in Riga and took place on 14–16 May.

The 32nd Spring Conference brought together more than 130 delegates and three organisations from 45 countries. Participants exchanged views on their supervisory activities and international cooperation, which are becoming increasingly important with advances in technology.

The FDPIC took part in a panel discussion on cooperation between EEA and non-EEA countries and the challenges posed by the fact that global tech companies process personal data across different economic zones.

ECHW

Workshops on practical cases

The European Case Handling Workshop (ECHW) is a sub-working group of the Spring Conference which brings together experts annually to discuss supervision cases. The ECHW 2024 event was hosted by the Estonian data protection authority in Tallinn and took place on 5–6 December.

Topics discussed during the workshops included cases involving the use of video cameras in public areas and apartment buildings, the use of data protection impact assessments and the definition of personal data in social media. The FDPIC representative presented a case study on facial recognition cameras in public spaces covering aspects of comparative law.

OECD

Working Party on Data Governance and Privacy in the Digital Economy

The OECD conducts research and analysis in the field of data governance and is at the forefront of the global debate on data protection focusing on the latest developments and challenges. In particular, it seeks to strengthen trust in cross-border data transfers and ensure a secure and efficient system. The OECD fosters a global digital environment that allows secure, seamless data flow across international borders.

One of the OECD's key priorities is to ensure a high level of data protection and data control, particularly in cross-border data transfers. The OECD is working to develop standards and guidelines that provide the necessary data security while supporting innovation and the free flow of information. Its ultimate goal is to help build a trustworthy and transparent framework that will make it possible to realise the full potential of digital technologies while protecting the rights and freedoms of users.

Working Party on Data Governance and Privacy

The FDPIC is represented in the OECD Working Party on Data Governance and Privacy in the Digital Economy (DGP). The working party reports to the OECD Committee on Digital Economy Policy (CDEP) and is composed of delegates from the 38 OECD Member States, including, in particular, representatives of governments and data protection authorities. It works with other CDEP working parties and other OECD committees to develop and promote evidence-based policies on data governance and privacy with a view to maximising the social and economic benefits from the wider and more effective use of data while, at the same time, addressing related privacy risks and challenges.

One of the key areas that the DGP focused on was analysing government access to private-sector data allowing the efficient discharge of public duties while ensuring effective data protection. The DGP also explored the complex interplay between different digital regulatory frameworks in order to create coherent and efficient governance structures. The working party also discussed the role of trusted data intermediaries, i.e. neutral third parties with the role of facilitating a secure and efficient data-sharing environment. Key topics were the integration of artificial intelligence (AI) in digital systems and the importance of privacy-enhancing technologies (PETs). The DGP also addressed the dynamics of cross-border payments with a view to improving the efficiency and security of these transactions in today's global economy. The aim is to map the interaction between data governance, data protection legislation and financial regulations relating to cross-border payments in order to provide data protection authorities with a better understanding of how the sector works and the compliance challenges it faces.

SYMPOSIUM

Privacy Symposium in Venice

The Privacy Symposium focused on mass data scraping, data protection in humanitarian action, and regional and international cooperation.

With over 300 authorities and experts sharing their perspectives, the Privacy Symposium provides a forum for data protection professionals, experts, authorities and researchers.

The FDPIC took part in a number of panels on the following topics:

- Data scraping: cosignatories of the Joint Statement on Data Scraping with other data protection authorities, (see text on data scraping above);
- Data protection in humanitarian action in the presence of international organisations and data protection authorities (see text on WG AID): The panellists explored the relationship between data protection and humanitarian action, from aiding disaster response to tracking displacement trends, where data plays a crucial role in shaping effective humanitarian interventions;
- The importance of regional and international cooperation: The panellists discussed how to strengthen existing cooperation, particularly between non-EU European authorities.

The Privacy Symposium aims to promote international dialogue, cooperation and knowledge sharing on data protection, compliance and emerging technologies. The 2024 edition of the Privacy Symposium took place in Venice, Italy, from 10 to 14 June under the patronage of the Italian data protection authority (the Garante).

GPA

Protecting privacy in the digital age

The theme for the 46th Global Privacy Assembly centred around the power of information. Four resolutions on key issues were adopted at the annual conference.

Under the central theme «The Power of i», the Global Privacy Assembly (GPA) focused on eight important themes: individuals, innovation, information, integrity, independence, international, intercultural and indigenous.

The open session explored how we can respect and balance the power of information with the need for citizens to have control over their personal information. The topics discussed included defining privacy harms, data protection and mental health, the impact of technology on regulatory authorities, and the advantages and challenges of data transfer tools. The participants also discussed the role of data privacy in humanitarian crises, reducing inequalities in privacy rights (exploring the different privacy dimensions of diversity), and data sharing between government and third parties among other subjects. This

constructive dialogue aimed to strengthen the effectiveness of current legal models and to promote ways to improve them in line with technological changes.

During the closed session, the GPA adopted four resolutions:

- Resolution endorsing and encouraging the use of data protection certification mechanisms;
- Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology;
- Resolution on data free flow with trust and an effective regulation of global data flows;
- Resolution on the GPA rules & procedures.

The Global Privacy Assembly, of which the FDPIC is a member, was established in 1979. It brings together data protection authorities from more than 100 countries to discuss key privacy issues and how regulators can work effectively – both individually and collectively – to protect privacy in an increasingly data-driven world. Its 46th Annual Conference was held in St. Helier, Jersey, from 29 October to 1 November 2024.

AFAPDP

New chair and updated Articles of Association

The members of the Association of Francophone Data Protection Authorities (AFAPDP) have elected a new chair and adopted new Articles of Association. Also on the agenda: support for the Madagascan authorities in setting up a dedicated commission.

At their General Assembly, the members unanimously elected Mauritius data protection commissioner Drudeisha Madhub as the new chair. The first woman to head the network, she is also the first representative of the Africa-Indian Ocean region since the AFAPDP was founded.

GPA – GT AID

Advancing privacy protection in emergency situations

Chaired by the FDPIC, the GPA's working group WG AID (dedicated to humanitarian action) stepped up efforts to raise awareness about privacy protection in emergency situations. It held a panel discussion on the subject at the Privacy Symposium in Venice and participated in the review of the third edition of the ICRC Handbook on Data Protection in Humanitarian Action. As part of its work to advance privacy protection worldwide, it took part in several panels including that of the International Organisations Workshop on Data Protection co-hosted by the EDPS and the World Bank. The group also drew up a list of African countries with data protection legislation and a data protection authority, including contacts within the authorities.

The FDPIC participated in a working group to update the association's Articles of Association – dating back to 2013 – which were then adopted.

The members also discussed supporting the Madagascan authorities with regard to the protection of personal data in the project launched by the Organisation internationale de la Francophonie with the aim of modernising Madagascar's civil status system. In particular, this involves helping to set up the Malagasy Commission on Information Technology and Civil Liberties (CMIL).

The AFAPDP brings together independent data protection authorities from 26 States (including Switzerland) which share a common language, values and legal tradition. The 16th General Assembly was held in St. Helier, Jersey, on 28 November 2024.

BILATERAL MEETINGS

Discussions with counterparts

During the year under review, the FDPIC received two foreign delegations in Berne to discuss common challenges and bilateral cooperation.

In June 2024, the Commissioner met with his newly appointed Austrian counterpart, Matthias Schmidl, to exchange views. The commissioners discussed common challenges and bilateral cooperation in the field of digitalisation and data protection as well as freedom of information and the principle of transparency.

In August 2024, the FDPIC met with his Somali counterpart, Mohamed Ali, Somalia's first data protection commissioner. The Somali Data Protection Act was adopted in March 2023. During their exchange, the two commissioners discussed the new data protection authority's initial experiences and the general challenges of data protection law in a digitalised world.

Freedom of Information

2.1 General

The Freedom of Information Act seeks to promote transparency with regard to the mandate, organisation and activities of the Administration by ensuring access to official documents (see Article 1 FoIA). In applying the principle of freedom of information, the Administration aims to increase confidence in the State and the authorities by creating a greater understanding and, consequently, acceptance of their actions.

The figures provided by the Federal Administration regarding the number of applications received in 2024 for access to official documents indicate that the media and society's need for specific information and transparent administration (including transparency regarding the activities of the Administration) is as strong as ever, with applications reaching an all-time high. During the year under review, the number of applications for access received by the federal authorities was almost 30 % higher than the previous year. According to the authorities, the amount of time required to process the applications has increased accordingly. Overall, implementing freedom of information has again proved to be a demanding and challenging task. The figures in Section 2.2 below show a continuation this past reporting year of the trend observed in recent years, namely a consistently high proportion of cases in which access was granted in full.

If the applicants or third parties affected by the access granted disagree with the authorities' decision to grant access, the Freedom of Information Act entitles them to submit a mediation request to the FDPIC. In 2024, the FDPIC received the largest number of mediation requests since the Freedom of Information Act came into force, namely 202, i. e. 53 % more than the previous year. The purpose of mediation is to enable a swift agreement between the parties. Oral mediation sessions in situ proved beneficial again in 2024: where a mediation session was held, an amicable solution was reached in 76 % of cases.

The consistently large number of mediation requests in recent years and the increasing complexity of the legal issues involved have created a backlog of procedures awaiting completion. As a result, the FDPIC exceeded the statutory processing time of 30 days in 72 % of cases. This negative trend is likely to worsen, making swift processing, as required by law, increasingly difficult to achieve (see Section 2.3 for more details).

At the beginning of 2025, another unpleasant situation arose when an applicant – a local politician – failed to attend a mediation session without excusing himself. The FDPIC deplores

this negligence, which resulted in unnecessary work and time being spent by him, his legal staff and the competent authority. If an applicant is absent without excuse, mediation proceedings are dismissed by law.

There was also a rather unpleasant case in which an authority failed to honour the written agreement made with the applicant during the mediation session. If an authority fails to fulfil its contractual obligation, the applicant can take legal action through the Federal Administrative Court to obtain the agreed access to the official documents.

2024 saw further efforts by the Administration to exclude more areas of its activities and certain categories of documents from the Freedom of Information Act. An overview of the special provisions under Article 4 FoIA can be found in Section 2.5.

In particular, the Federal Council excluded the Swiss Transportation Safety Investigation Board (STSB) from the scope of the Freedom of Information Act based on Article 2 paragraph 3 FoIA (see Section 2.4). In the FDPIC's view, the key problem here is that the Administration is exempting itself from the principle of transparency within the Administration, effectively preempting an upcoming decision by the legislator as part of the partial revision of the Federal Aviation Act. Furthermore, the FDPIC disputes the need for this unconditional restriction of the Freedom of Information Act. Introducing reservations of this sort undermines the principle of freedom of information and the transparency within the Administration that the principle seeks to achieve.

Overall, however, most areas of the Administration have embraced and are actively implementing the paradigm shift from the principle of secrecy to one of transparency brought about by the Freedom of Information Act.

2.2 Applications for access: sharp increase in 2024

According to the figures released, the federal authorities received 2186 applications for access to information during the year under review, i. e. 29 % more than in 2023 (1701). In 2024, they also processed 46 applications for access that had been submitted in previous years. Full access was granted in 1159 cases (52 %), compared with 830 (48 %) in 2023. In 474 cases (21 %), access to the documents requested was partially granted or deferred, compared with 402 (23 %) the year before. In 179 cases (8 %), access was denied outright, compared with 176 cases (10 %) in 2023. According to the authorities, 133 applications for access were withdrawn (6 %) (compared with 73 (4 %) the previous year), 102 applications were still pending at the end of 2024, and in 185 cases there was no official document.

In summary, the FDPIC notes that, during the year under review, full access to the documents requested was granted in more than 50 % of cases. With the exception of last year, this long-term trend appears to have been confirmed in 2024. The number of applications for access that were denied outright remains low, having stabilised at just under 10 % in recent years.

Federal departments and federal offices

Several administrative units were the focus of particular media and public interest in 2024. Due to the nature of their work, the DDPS (527), DETEC (324) and FDFA (306) received large numbers of applications for access to information. According to the authorities, the applications received were sometimes very extensive and complex, often requiring time-consuming coordination between federal offices and departments.

The figures released by the federal offices indicate that the FOSPO received the most applications for access in 2024, namely 317, followed by the ETH Domain with 143, the FOEN with 139 and the FCh with 94. Seven authorities reported receiving no applications for access during the year under review. The FDPIC himself received 29 applications for access and granted full access in 18 cases; access was denied outright in one case, and partial access was granted in four cases. Six applications were still pending at the end of 2024.

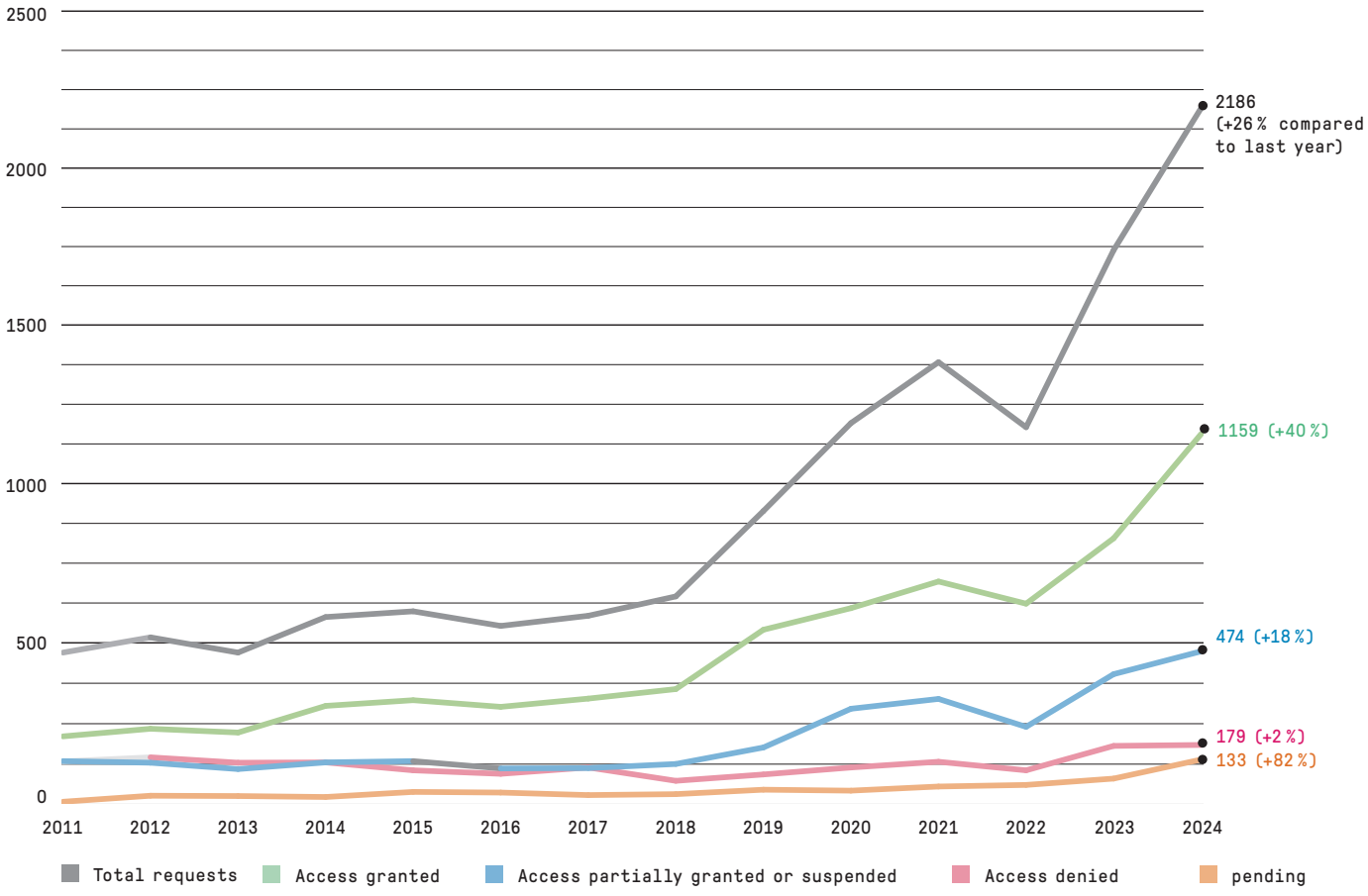
In 2024, fees charged for access to official documents totalled CHF 9,950.00, a hefty 30 % lower than the previous year (CHF 14,226.20). While the FCh, the FDFA, the FDJP, the DDPS, the Parliamentary Services and the Office of the Attorney General of Switzerland charged no fees, the other four departments did invoice applicants for some of the time spent dealing with their applications (FDHA: CHF 4,250.00; EAER: CHF 3,6000.00; FDF: CHF 2,000.000; DETEC: CHF 100.00).

It should be noted that just seven of the 2232 applications processed incurred a fee. Compared with the previous year, when fees were charged in 19 cases, both the number of cases in which a fee was charged and the total amount charged were significantly lower. Fee-charging remains the exception (0.3 %). The Administration's practice of granting cost-free access to official documents in principle was enshrined in the Freedom of Information Act on 1 November 2023. By way of exception, authorities may charge fees for applications that requires disproportionate effort to process.

The FDPIC points out that the authorities are under no obligation to record the time they spend processing applications for access to information and that there are no legal requirements in terms of a standard recording procedure applicable throughout the Federal Administration. Data is sent to the FDPIC on a purely voluntary basis and therefore reflects only a portion of the time actually spent processing applications. However, according to the data received, the time spent this past reporting year increased further to 7,256 hours, up from 2023 (6,469 hours).

The fact that the time spent processing applications reported by the authorities reflects only a portion of the actual time required is illustrated, for example, by the data provided by the FOPH. In addition to the 482 working hours reported by the FOPH's specialist units, the FOPH reported a large amount of time (amounting to at least 3.6 FTEs)

Figure 1: Evaluation of applications for access – trend since 2011




3 Institutsarbeiten

spent processing applications (including mediation and appeal procedures) and providing legal support through its freedom of information advisor. The same may apply to other authorities.

The time spent preparing mediation proceedings also increased significantly, totalling 1,271 hours, compared with 730 hours last year, 1,006 hours in 2022, 865 hours in 2021 and 569 hours in 2020.

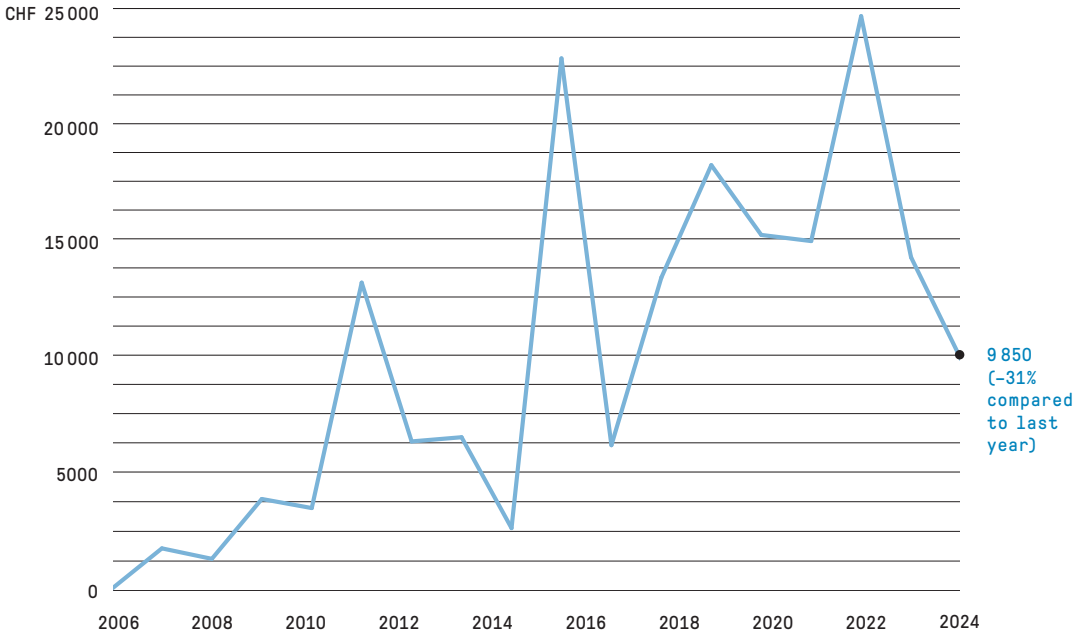
Parliamentary Services

The Parliamentary Services reported receiving five applications for access during the year under review. Access was granted in full in one case, and partial access was granted in another. Access was denied outright in two cases, and in one case there was no official document.

Office of the Attorney General of Switzerland

The Office of the Attorney General of Switzerland reported receiving eight applications for access in 2024. It granted full access in three cases and denied access altogether in two other cases. Three applications were still pending at the end of 2024.

Figure 2: Fees charged since the FoIA entered into force



2.3 Mediation proceedings – significant increase in the number of mediation requests

In 2024, the FDPIC received the highest number of mediation requests since the Freedom of Information Act came into force, namely 202, i. e. 53 % more than in 2023 (132 requests). The majority of mediation requests were filed by private individuals (66) and the media (61). Therefore, of the 838 cases in which the Federal Administration fully or partially denied access, deferred access or stated that there were no official documents, 202 cases (24 % of all unmet applications for access) resulted in a mediation request being submitted to the FDPIC.

In 2024, 157 mediation requests were settled (another all-time high), 130 of which had been submitted during the same reporting year, and 27 the previous year. In 92 cases, the participants were able to reach an agreement. The FDPIC also issued 31 recommendations, which enabled 32 cases to be resolved in which no amicable solution between the parties involved was apparent.

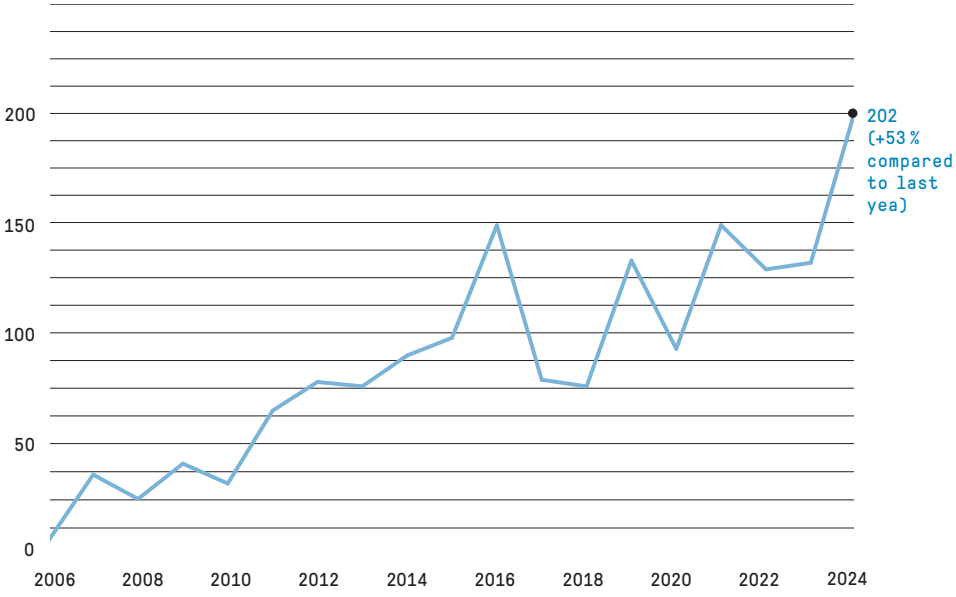
The cases dealt with include 15 mediation requests which had not been submitted on time, ten cases which did not satisfy the conditions for application of the Freedom of Information Act, and eight requests for mediation that were withdrawn. Ten mediation proceedings were suspended by agreement between the participants or at their request.

Proportion of amicable outcomes

There are numerous advantages to amicable solutions: For instance, they are an opportunity to clarify the facts, accelerate the procedure for access to documents and establish the bases for possible future collaboration among the participants.

The ratio of amicable outcomes to recommendations is the best measure of the effectiveness of oral mediation sessions. During the year under review,

Figure 3: Mediation requests since the FoIA entered into force



92 amicable outcomes were achieved, and the FDPIC issued 30 recommendations to settle 32 cases. Therefore, the ratio of amicable outcomes to recommendations is 74 %. In the 82 mediation sessions that took place during the year under review, an agreement was reached in 62 cases (76 %).

This clearly shows that oral mediation by the FDPIC is effective in reaching amicable solutions. Oral mediation sessions have proven beneficial for all participants and should therefore be maintained.

Note: All the recommendations issued in the year under review are available on the FDPIC's website (www.edoeb.admin.ch).

Table 1: Amicable outcomes

2024	74 %
2023	47 %
2022 (Corona-19)	51 %
2021 (Corona-19)	44 %
2020 (Corona-19)	34 %
2019	61 %
2018	55 %

Duration of mediation proceedings

Table 2 is divided into three sections according to processing time, whereby the processing time indicated does not include the period of time during which a mediation proceeding is suspended at the participants' request or with their consent. A mediation proceeding is typically suspended when an authority wishes to review its position after the mediation session or has to consult third parties involved. Also, if a mediation session is postponed at the request of one of the parties (due to holidays, illness etc.), the processing time does not include the period of time by which the proceedings are extended.

The table shows that 28 % of mediation proceedings completed in 2024 were concluded within the 30-day period, while 45 % took between 31 and 99 days, and 27 % took 100 days or longer.

In just 16 (36 %) of the 44 mediation requests settled within the 30-day period, the mediation proceedings were settled following a discussion of the issues that were the subject of mediation. In the other 28 cases (64 %), no substantive assessment was made. These were mainly cases that clearly fell outside the scope of the Freedom of Information Act or in which the formal requirements for initiating mediation were not met.

Mediation proceedings took longer again because of the processing backlog from previous years and the large number of new requests in 2024. In addition, the number of mediation requests received is typically subject to fluctuation. For example, the FDPIC received a large number of requests in June (30) and October (26) but only eight in August and nine in December.

Before the pandemic, the statutory 30-day deadline for completing a mediation proceeding was regularly met when the mediation sessions culminated in agreement. This was not the case in

the year under review. Nevertheless, when the mediation sessions culminated in agreement, the 30-day deadline was met in 20 % of cases compared with 35 % the previous year. The backlog and the limited human resources available for processing mediation requests meant that in 95 % of cases it was clear that the deadline would already have expired by the time the mediation sessions were due to take place. When an amicable solution could not be reached and the FDPIC had to issue a written recommendation to the parties involved, he was unable to do so at all within the statutory period of 30 days from receipt of the mediation request.

Failure to meet the deadline was also due to particularly extensive applications for access to documents, large numbers of third parties involved in a procedure, and complex legal issues. Cases such as these frequently entail a particularly high workload, and so in such cases – in accordance with Article 12a of the Freedom of Information Ordinance (FoIO; RS 152.31) – the FDPIC may extend the deadline by an appropriate period of time.

While exceeding the tight deadline of 30 days in complex cases and in procedures involving several parties (i. e. several third parties affected) is regarded as inherent in the system given the possibility of extension provided for by law, the further increase in the number of cases in which deadlines were exceeded – which can only be explained by the large increase in the number of mediation requests – constitutes undue delay from a legal standpoint.

Table 2: Precessing time of mediation proceedings

Processing time in days	2014 – August 2016*	Pilot phase 2017	2018	2019	2020	2021	2022	2023	2024
within 30 days	11 %	59 %	50 %	57 %	43 %	42 %	25 %	27 %	28 %
between 31 and 90 days	45 %	37 %	50 %	38 %	30 %	51 %	42 %	35 %	45 %
100 days and more	44 %	4 %	0 %	5 %	27 %	7 %	33 %	38 %	27 %

* Source: Presentation by the Commissioner, event marking the 10th anniversary of the FoIA, 2 September 2016

Number of pending cases

The figures in Table 3 indicate the number of pending cases at the end of the reporting years shown. At the beginning of January 2025, 66 mediation proceedings were still pending, including ten suspended proceedings (one from 2019, one from 2021, two from 2022, and six from the year under review). Nineteen cases had been completed by the time of going to press.

Table 3: Pending mediation proceedings

End of 2024	**66 (19 completed by the time of going to press and 10 suspended)**
End of 2023	31 (17 completed by the time of going to press and 9 suspended)
End of 2022	41 (16 completed by the time of going to press and 13 suspended)
End of 2021	27 (14 completed by the time of going to press and 8 suspended)
End of 2020	17 (9 completed by the time of going to press and 8 suspended)
End of 2019	43 (40 completed by the time of going to press and 3 suspended)
End of 2018	15 (14 completed by the time of going to press and 2 suspended)

2.4 Legislative process

CC-S REPORT

Federal Council refuses to consider granting the FDPIC a right to issue rulings

In its report on untraceable emails in the General Secretariat of the Federal Department of Home Affairs (FDHA), the Control Committee of the Council of States (CC-S) stated that the rules for filing and archiving documents within the Federal Administration were inconsistent and needed clarifying. The Committee issued five recommendations and concluded, among other things, that the FDPIC's rights to inspect official documents should be strengthened. The Federal Council issued a report in which it assessed the five recommendations.

In its report of 10 October 2023 on the archiving and filing of documents and the procedure for applications for access to documents according to FoIA (in which it investigates the general requirements and the specific allegation of untraceable emails within the GS-FDHA), the CC-S examines the legal bases for the retention, filing and archiving of documents (Archiving Act) and access to official documents (Freedom of Information Act). The FDPIC has reported in detail on this matter in previous annual reports (see 31st Annual Report, Section 2.4, and 30th Annual Report, Section 2.4).

In its report, the Committee published five recommendations to the Federal Council, three of which are directly related to the Freedom of Information Act:

- In Recommendation 1, the Committee invites the Federal Council to assess the need to amend the legal requirements regarding the right of access to documents related to a federal employee's office that also contain information relating to their private life, with particular regard to Senior members of government.
- In Recommendation 4, the Federal Council is invited to assess whether the Freedom of Information Act is also (or should also be) applicable to concluded criminal proceedings and whether this should be specified in the next revision.
- In Recommendation 5, the Federal Council is invited to consider amending the Freedom of Information Act to grant the FDPIC a right of intervention or a right to issue rulings in the event that his right of inspection is not respected.

In its first response to the CC-S on 11 January 2024, the Federal Council stated that it fully accepted the assessments referred to in Recommendations 1-4. However, it refused to consider a right to issue rulings for the FDPIC as proposed in Recommendation 5 but was prepared to consider intervention rights for the FDPIC in the event that he was denied inspection rights.

The Federal Council then instructed the Federal Department of Justice and Police (FDJP) to review the recommendations by the end of 2024 and to submit a report outlining proposals for further action. The FDPIC commented on the draft report regarding the individual recommendations and the Federal Council's statements in a preliminary consultation and in an office consultation with the FDJP:

- Regarding Recommendation 1, the Federal Council stated that in the case of documents related to a person's office that also contain information relating to their private life, it should

always be assessed on an individual basis whether there is a right of access under the Freedom of Information Act or a right of inspection under the Archiving Act. It sees no need for legal amendments. The CC-S's Recommendation 1 addressed a specific aspect of coordination between the Archiving Act and the Freedom of Information Act and the corresponding inspection rights. However, the FDPIC took the view in the consultations that a full or partial revision of the legislative texts was unavoidable in order to regulate coordination between the Archiving Act and the Freedom of Information Act and achieve the necessary legal certainty, especially as the two inspection procedures differ significantly in terms of substantive and procedural law, which the Federal Council also recognises in principle in its report.

- With regard to Recommendation 4 and applicability of the Freedom of Information Act, we noted that our comments on Supreme Court case law had not been taken on board, namely that the Federal Supreme Court had already ruled on how Article 3 paragraph 1 letter a FoIA was to be applied. Based on a restrictive interpretation of the grounds for excluding the procedural documents mentioned in Article 3 paragraph 1 letter a of the Freedom of Information Act, the court had concluded that only procedural documents in the strict sense were excluded from the scope of the Freedom of Information Act. In terms of the requirements set by the court for such an exclusion, whether proceedings are still underway or have already been concluded is irrelevant. In the FDPIC's view, the question regarding access to procedural documents has thus been definitively clarified by the Federal Supreme Court.
- Regarding Recommendation 5, the Federal Council stood by its view expressed on 11 January 2024 and refused to consider granting the FDPIC a right to issue rulings. It argued that, under the Freedom of Information Act, the mediation proceeding was an informal, non-prejudicial procedure and that it would therefore be inappropriate for the FDPIC to have power of disposal. In the office consultation, the FDPIC stated that by refusing to consider granting a right to issue rulings, the Federal Council had failed to comply with the CC-S's request to examine not only the issue of the intervention rights for the FDPIC but also a specific right to issue rulings. Our request for a reassessment was rejected.

The Federal Council's report of 13 December 2024 submitted to the CC-S was adopted and published in the form proposed by the FDJP.

FEDERAL PERSONNEL LAW

Restricting freedom of information in connection with whistleblowing

The revised Federal Personnel Act currently being debated in Parliament introduces significant restrictions on freedom of information, particularly with regard to the handling of whistleblower reports. The FDPIC has repeatedly opposed the intended restriction of freedom of information.

On 28 August 2024, the Federal Council submitted the dispatch for the revised Federal Personnel Act (FPA) to Parliament. In addition to adjustments to occupational pensions, the revised act introduces measures designed to improve data protection in relation to profiling and the promotion of digitalisation in human resources (see Section 1.5). Finally, the Federal Council intends to introduce a number of changes in the revised act aimed at increasing efficiency in the implementation of federal personnel law.

As an efficiency measure, in Article 22a paragraph 7 of the draft Federal Personnel Act (draft FPA), the Federal Council proposes excluding from the scope of the Freedom of Information Act all documents that substantiate a report under Article 22a of the draft FPA (reports, notifications and protection in relation to whistleblowing), documents that are submitted along with a report, and documents that were created on the basis of a report. The Federal Office of Personnel (FOPER), which is responsible for the proposal, justifies the restriction of freedom of information by emphasising the need to foster long-term trust in the whistleblowing tool. Furthermore, restricting freedom of information for the above-mentioned documents would protect persons accused of unlawful behaviour according to whistblower reports.

In two consultation procedures and an interim consultation, the FDPIC pointed out, in vain, that justified private interests remained protected even when the Freedom of Information Act was applied. He explained that whistleblowing is already a highly trusted tool, especially since the whistleblowing provision in Article 22a FPA came into force on 1 January 2011. The reporting and notification obligations of federal employees in the event of official offences and the right to report other irregularities – enshrined in the act – have been actively used since the provision was introduced. Statistical analyses by the Swiss Federal Audit Office (SFAO) show a steady increase in the number of reports submitted. It is not clear to the FDPIC to what extent maintaining the current provision – without exclusion under Article 4 FoIA – could or would result in a loss of trust. Besides, in the FDPIC's view, the Freedom of Information Act offers sufficient measures to ensure the protection of sensitive information and personal data of persons who use the whistleblowing tool as well as those who could be affected by the reports (see Articles 7 and 9 FoIA). Therefore, the FDPIC does not consider it necessary to deny public access to all reports, including any enclosures, as well as all other documents that are created on the basis of such reports – including any outcome documents and final reports. This also

goes against the principle of proportionality set out in Article 5 paragraph 2 of the Federal Constitution. In the FDPIC's view, the proposed restriction of freedom of information cannot be justified given the legitimate public interest in a serious investigation of reported misconduct by employees of the Administration.

Finally, the FDPIC points out that whistleblowing offices should not be subject to state secrecy as they are required by law to scrutinise any reported administrative units and/or employees and are therefore very much in the public eye.

The legislative dispatch submitted by the Federal Council to Parliament, which is currently debating it, still includes the exclusion from the scope of the Freedom of Information Act, and the FDPIC's opposing view is accurately formulated.

AVIATION

Supervision of civil aviation to be excluded from Freedom of Information Act

The supervision of civil aviation is to be largely excluded from the scope of the Freedom of Information Act. During the office consultation and the consultation procedure, the FDPIC opposed the plan to restrict the freedom of information.

The consultation draft prepared by the Federal Office of Civil Aviation (FOCA) for an amendment to the Aviation Act provides for major restrictions on the freedom of information, particularly regarding legal supervision of the FOCA. According to Article 107d paragraph 2 of the consultation draft of the Federal Aviation Act (AViA), the Freedom of Information Act should not apply to access to personal data or data relating to legal entities or to the following official documents if granting access to them could jeopardise flight or aviation safety: reports on audits, inspections, assessments and reviews by the FOCA (let. a), reports and related documents on events received by the FOCA under Regulation (EU) No. 376/2014 (let. b), and official documents on safety investigations by the Swiss Transportation Safety Investigation Board (STSB) (let. c).

As a supervisory authority that is subject to the Freedom of Information Act, the FDPIC rejected the proposed provisions arguing that the Freedom of Information Act also offered sufficient safeguards for supervisory activities – including safety investigations – in order to ensure the protection of sensitive data (see Art. 7 and 9 FoIA). We also pointed out that the legislator had deliberately chosen not to introduce an exemption clause in the Freedom of Information Act regarding confidentiality between the supervisory authority and the supervised entity.

The FOCA sometimes justifies restricting freedom of information by arguing that the supervised entities will only fulfil their reporting obligations if they do not expect the information in question to be disclosed. This assumption – erroneous in the view advanced here – fails to consider the fact that in a state governed by the rule of law, compliance with legal duties to report and to provide information is a given. Furthermore, the FOCA fails to acknowledge that possible infringements by supervised entities do not constitute justifiable grounds for restricting the Freedom of Information Act. Moreover, the FDPIC considers the argument that the reports often contain technical details that are difficult for the general public to evaluate correctly to be untenable and presumptuous. Therefore, the FDPIC sees no

convincing justification for the FOCA's plan to deny public access to documents of the Administration altogether and to maintain unconditional secrecy in relation to many of its supervisory activities.

Furthermore, the FDPIC points out that authorities with supervisory, auditing, monitoring or inspection duties are very much in the public eye as they have a legal duty to inspect other administrative units and private individuals. In these sensitive areas it is all the more important that the FDPIC object when supervisory authorities seek to exclude themselves from the scope of the Freedom of Information Act on the basis of arguments such as 'risk of non-compliance with reporting obligations' or information being 'too complex for the general public'.

A similar plan to introduce comprehensive restriction of freedom of information had already been proposed in the partial revision 1+ of the Federal Aviation Act back in 2014/2015. The FDPIC had firmly opposed the plan (see 22nd Annual Report, Section 2.2.2), which was later dropped. The FOCA has not explained how any changes in the meantime could justify placing greater restrictions on public access to documents of the Administration.

As the FOCA was not prepared to share the FDPIC's opposing views publicly in its explanatory report on the draft legislation after the office consultation, the FDPIC felt compelled to express his views in the consultation process as well for reasons of transparency.

AVIATION

Amendment of the Ordinance on the Safety Investigation of Transportation Incidents (OSITI)

With the amendment that came into force on 1 January 2025, the Federal Council excluded the Swiss Transportation Safety Investigation Board (STSB) from the scope of the Freedom of Information Act. The FDPIC had unsuccessfully opposed this restriction of the freedom of information in the office consultation. Under Article 2 paragraph 3 letter a FoIA, the Federal Council may exclude units of the Federal Administration from the personal scope of the Freedom of Information Act if the tasks assigned to them so requires. Availing itself of this option, it stipulates in the new Article 54a of the Ordinance on the Safety Investigation of Transportation Incidents (OSITI) that the STSB is excluded from the scope of the Freedom of Information Act insofar as it processes data of natural persons or legal entities.

The Federal Department of the Environment, Transport, Energy and Communications (DETEC), which is

responsible for amending the ordinance, justifies the need to exclude the STSB from the Freedom of Information Act on the grounds that the STSB will only receive information relevant to maintaining transportation safety if the reporting parties do not need to fear that the information will be disclosed. This argument is put forward again and again by the Federal Administration to justify the (apparent) need for restrictions on transparency within the Administration. As the FDPIC has already stated on several occasions, this justification is not convincing (see also the text above on the revision of the AviA as well as the 31st Annual Report, Section 2.4, and the 22nd Annual Report, Section 2.2.2). Furthermore, DETEC has not explained why the exemption provisions of the Freedom of Information Act should not be sufficient to ensure performance of the STSB's duties.

With the Federal Council's decision to exclude the STSB from the personal scope of the Freedom of Information Act, the Administration is effectively exempting itself from transparency within the Administration. This is all the more astonishing as the FOCA and the DETEC are already proposing the introduction of a special statutory provision as part of the partial revision of the AviA (see above) – and, therefore, at the legislative level – that would exclude the STSB from the scope of the Freedom of Information Act. In doing so, the Federal Council is preempting the parliamentary decisionmaking process.

However, after the exclusion of the STSB under Article 54a OSITI came into effect on 1 January 2025, the DETEC stated in the explanatory notes accompanying the provision that it was merely provisional as decisions on restrictions to the principle of transparency should in principle be reserved for the legislature.

FINANCIAL SUPERVISION

New federal act on the transparency of legal entities

Under new legislation on the transparency of legal entities, a central register is to be set up listing the beneficial owners of legal entities. Despite the FDPIC's intervention, the draft legislation provides for exemption from the Freedom of Information Act.

On 22 May 2024, the Federal Council submitted to Parliament a dispatch for a new Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (TLEA). The Act provides for the introduction of a register containing up-to-date information on the beneficial owners of the legal entities listed with a view to further strengthening the system for combating money laundering, terrorist financing and financial crime.

To the FDPIC's regret, following the consultation procedure (see 31st Annual Report, Section 2.4), the Federal Council included in the bill an expressed exemption from the Freedom of Information Act: Article 53 paragraph 4 of the bill states that the Freedom of Information Act shall not apply to data in the transparency register relating to natural persons or legal entities.

The State Secretariat for International Finance (SIF), which is responsible for the proposal, justifies restricting freedom of information on the grounds that the prime purpose of the transparency register is to strengthen the fight against money laundering and terrorist financing. The SIF sees no added value in opening up the register further and believes that doing so would constitute a disproportionate encroachment on personal privacy.

In the consultation procedure, the FDPIC pointed out, in vain, that justified private interests remained protected even when the Freedom of Information Act was applied. The Act explicitly guarantees the protection of business secrets (Art. 7 para. 1 let. g FoIA) and of the privacy and personal data of natural persons and legal entities (Art. 7 para. 2 FoIA, Art. 9 para. 2 FoIA in relation to Art. 36 FADP and Art. 57f GAOA). The FDPIC also pointed out that the right of access under the Freedom of Information Act also typically included databases and registers used by the authorities in the discharge of their public duties. In the FDPIC's view, to regulate this differently for the transparency register without sufficient justification defeats the purpose of the system and the concept behind it.

The draft submitted to Parliament by the Federal Council and currently undergoing parliamentary deliberation still contains the exemption from the Freedom of Information Act. It should be mentioned that the FDPIC's position was included in the Federal Council's dispatch.

EMERGENCY LAW

Application of emergency law: Federal Council report

In its postulate report of 19 June 2024, the Federal Council concludes that freedom of information is particularly important in times of crisis, and access to information should only be refused in exceptional circumstances. The FDPIC's position was presented in the report.

Over the past two decades, the Federal Council has repeatedly exercised its right to issue emergency ordinances based on the Federal Constitution in the event of impending crises (see Article 184 paragraph 3 and Article 185 paragraph 3 Cst.). In connection with the financial backstop for the electricity industry and the UBS takeover of Credit Suisse, it used the same emergency law to exclude the activities assigned to the Administration from the scope of the

Freedom of Information Act. Parliament instructed the Federal Council to clarify the legal basis and scope of emergency law and to assess the need for any amendments.

In its report of 19 June 2024, the Federal Council concludes that the right of access to information enshrined in the Freedom of Information Act should be refused under emergency law only in exceptional circumstances. In the Federal Council's view, this instrument – introduced by the legislator to enable citizens to scrutinise the actions of the Administration – is particularly important in times of crisis. Restricting the right of access therefore necessitates strong justification.

As part of the office consultation, the FDPIC commented on the draft report of the Federal Office of Justice (FOJ). In particular, he called for the deletion of two passages containing a legal assessment of legal issues that had not yet been clarified. In his statement, he also criticised (again) the justification given in the report for restricting the scope of the Freedom of Information Act on the grounds that compliance with statutory reporting obligations could otherwise not be guaranteed (see text on revised AViA, 31st Annual Report, Section 2.4, and 22nd Annual Report, Section 2.2.2). The FDPIC welcomes the implementation of the requested changes and the inclusion of his views in the report.

In his statement of 6 April 2023, the FDPIC had already pointed out that the justification provided for enacting emergency legislation in order to support the electricity or financial sectors did not explain the need to exclude by emergency legislation the rights of citizens to access information under the Freedom of Information Act. He reiterated this view in his recommendations of 27 November 2023 regarding access to documents relating to the UBS takeover of Credit Suisse. Finally, it should be noted that in its report of 17 December 2024 on government handling of the Credit Suisse crisis, the Parliamentary Investigation Committee (PInC) expressed doubts regarding the proportionality of denying access to documents of the Administration. It recommends that the Federal Council also apply the Freedom of Information Act when enacting emergency legislation (Recommendation no. 17 of the report).

2.5 Special reservations under Art. 4 FoIA

The Freedom of Information Act needs to be coordinated with the provisions of special federal laws that establish special rules for access to official documents. According to Article 4 FoIA, special provisions contained in other federal acts are reserved where they declare certain information secret (let. a) or declare the access to certain information to be subject to requirements derogating from those set out in the FoIA (let. b), thereby rendering the provisions of the FoIA inapplicable to access to such information.

Whether a legal provision takes precedence in the sense of a special provision pursuant to Art. 4 FoIA must be determined for each specific case by interpreting the relevant provisions.

Table 4: Special provisions under Art. 4 FoIA

Legislation (short form) and abbreviation	SR no.	Art./Para.	Entry into force:
Information Security Act (ISA)	128	Art. 4 para. 1 bis	(still open)
Dispatch regarding the amendment of the Federal Personnel Act (FPA)	177.220.1	Art. 22a para. 7 E-BPG	Dispatch dated 28 August 2024 Status: under discussion in parliament
Dispatch regarding the bill on the transparency of legal entities (LETA)		Art. 53 para. 4 FoIA	Dispatch dated 22 May 2024 Status: under discussion in parliament
Amendment to the Federal Health Insurance Act HIA (Cost containment measures – Package 2)	832.10	Art. 52c HIA (delegation norm) Art. 52d para. 5 HIA Transitional provision HIA para. 4	Adopted by Parliament on 21 March 2025.
	831.20	Art. 14^{quinquies} para. 2 and 3 InvIA (delegation norm) Art. 14^{sexies} para. 5 InvIA Transitional provision InvIA para. 1	
Federal Act on Subsidiary Financial Aid to Support Systemically Critical Companies in the Electricity Industry (FiRECA)	734.91	Art. 20 para. 4	1 October 2022
Federal Act on Public Procurement (PPA)	172.056.1	Art. 48 para. 1 (explicit access provided); Art. 11 let. e (only considered a special provision during award procedures)	1 January 2021
Covid-19 Loan Guarantees Act	951.26	Art. 12 para. 2	19 December 2020
Federal Act on the Organisation of the Railway Infrastructure (OBI in German) (consolidation bill)			
Railways Act (RailA)	742.101	Art. 14 para. 2	1 July 2020
Cableways Act (CabA)	743.01	Art. 24e	1 July 2020
Passenger Transport Act (PTA)	745.1	Art. 52a	1 July 2020
Federal Act on Inland Navigation (INA)	747.201	Art. 15b	1 July 2020
Intelligence Service Act (IntelSA)	121	Art. 67	1 September 2017
Foodstuffs Act (FoodA)	817.0	Art. 24 Special provision in accordance with the dispatch on the Federal Act on Foodstuffs and Utility Articles of 25 May 2011	1 May 2017

Legislation (short form) and abbreviation	SR no.	Art./Para.	Entry into force:
Federal Act on the Promotion of Research and Innovation (RIPA)	420.1	Art. 13 para. 4 (see FAC ruling A-6160/2018 of 4 November 2019 E. 4)	1 January 2014
Banking Act (BankA)	952.0	Art. 47 para. 1	1 January 2009 (let. a and b) and 1 July 2015 (let. c)
Patents Act (PatA)	232.14	Art. 90 PatO based on Art. 65 para. 2 PatA (see FSC ruling 4A_249/2021 of 10 June 2021)	1 July 2008
Patents Ordinance (PatO)	232.141		
Entry into force of the Freedom of Information Act			**1. July 2006**
Parliament Act (ParlA)	171.10	Art. 47 para. 1 (see FAC ruling A-6108/2016 of 28 March 2018 E. 3.1)	1 December 2003
Goods Control Act (GCA)	946.202	Art. 4 and 5 (see FAC ruling A-5133/2019 of 24 November 2021 E. 5.3.2.4)	1 October 1997
Federal Act on Direct Federal Taxation (DFTA)	642.11	Art. 110 para. 1	1 January 1995
Withholding Tax Act (WTA)	642.21	Art. 37 para. 1	1. January 1967
Federal Act on Stamp Duties (StA)	641.10	Art. 33 para. 1	1 July 1974
VAT Act (VATA)	641.20	Art. 74 para. 1 (see FSC ruling 1C_272/2022 of 15 November 2023 E. 3.4)	1 January 2010
Direct Taxation Harmonisation Act (DTHA)	642.14	Art. 39 para. 1 (see ACLFA 2016.1 (pp.1 – 14), issued on 26 January 2016: Tax secrecy and access to official documents)	1 January 1993
Federal Statistics Act (FStatA)	431.01	Art. 14 (see FSC ruling 1C_50/2015 of 2 December 2015 E. 4.2. ff.)	1 August 1993

Table 5: NO special provisions under Art. 4 FoIA

Legislation (short form) and abbreviation	SR no.	Art./Para.	Entry into force:
Federal Act on Product Safety (ProdSA)	930.11	Art. 10 para. 4 in conjunction with Art. 12 (see FSC ruling 1C_299/2019 of 7 April 2020 E. 5.5)	1 July 2010
Auditor Oversight Act (AOA)	221.302	Art. 19 Para. 2 (see FSC ruling 1C_93/2021 of 6 May 2022 E. 3.6)	1 September 2007
Telecommunications Act (TCA)	784.10	Art. 24f (s. Judgement of the FAC A-516/2022 of 12 September 2023 E.)	1 April 2007
Federal Act on General Aspects of Social Security Law (GSSLA)	830.1	Art. 33 (No special provisions under Art. 4 FoIA in this case: see FAC ruling A-5111/2013 of 6 August 2014 E. 4.1 ff. and A-4962/2012 of 22 April 2013 E. 6.1.3)	1 January 2003
Therapeutic Products Act (TPA)	812.21	Art. 61 und 62 (see FSC ruling 1C_562/2017 of 2 July 2018 E. 3.2 and FAC ruling A-3621/2014 of 2 September 2015 E. 4.4.2.3 ff.)	1 January 2002
Federal Act on Occupational Old Age, Survivors' and Invalidity Pension Provision (OPA)	831.40	Art. 86 (see FSC ruling 1C_336/2021 of 3 March 2022 E. 3.4.3)	1 January 2001

The FDPIC

3.1 Duties and resources

Services and resources in the field of data protection

Number of staff

The number of staff employed by the FDPIC to deal with data protection issues since 2023 – the year in which the FADP came into force – remains unchanged at 33 full-time positions.

Table 6: Staff positions available for FADP issues

2023	33
2024	33
2025	**33**

Services

The FDPIC's duties as the data protection authority for the federal authorities and the private sector have been divided into four service groups in line with the New Management Model for the Federal Administration (NMM): consultancy, supervision, information and legislation. During the reporting year running from 1 April 2024 to 31 March 2025, the FDPIC's staff resources available for data protection were allocated to these four groups as follows:

Table 7: Services in data protection

Consultancy – Federal Administration	20,8 %	
Consultancy – private individuals	18,0 %	
Cooperation with foreign authorities	15,1 %	
Cooperation with cantons	1,2 %	
Total consultancy		**55,1 %**
Supervision	20,2 %	
Certification	0,1 %	
Total supervision		**20,3 %**
Information	12,5 %	
Training, talks and presentations	2,6 %	
Total Information		**15,1 %**
Legislation	9,5 %	
Total legislation		**9,5 %**
Total data protection		**100,0 %**

Consultancy

The FDPIC faces a consistently high demand for consultancy services as he is legally required to support large-scale digital projects. He has an advisory role both within the Federal Administration – e. g. in the CEBA (see Section 1.1), POLAP (see Section 1.2), Zurich Airport facial recognition (see Section 1.6) and Justitia 4.0 (see Section 1.1) projects – and vis-à-vis public (SBB, Swisscom, see Section 1.6) and private companies. As part of these projects, the FDPIC often reviews data protection impact assessments. During the year under review, the proportion of staff working in consultancy amounted to 55.1 %, marginally higher than last year (53.3 %).

The above suggests the following outcome objectives against which resources should be measured, broken down by outcome group:

Table 8: Outcome objectives for FDPIC in data protection

Service group	Outcome objectives
Consultancy	The consultancy the FDPIC provides for individuals and for businesses and federal authorities running projects involving sensitive data meets general expectations.
Supervision	The frequency of FDPIC inspections is credible.
Information	The FDPIC proactively raises public awareness of the risks posed by individual digital technologies and their usage. He has a contemporary, user-friendly website available to the general public as well as online reporting portals.
Legislation	The FDPIC has an early say on and actively influences all special rules and regulations created at national and international level. He helps the parties involved to formulate rules of good practice.

Supervision and campaigns

The number of complaints handled by the three teams in the Data Protection Directorate during the year under review totalled 1,053. At 20.3 %, the proportion of resources allocated to inspections and supervisory procedures was significantly higher than the average of 15 % for the reporting years since 2015. The FDPIC was thus able to strengthen his supervisory activities in line with his strategic goals, which is reflected in the statistics. The table below shows the number of low-threshold interventions, preliminary investigations and formal investigations.

Two campaigns were carried out in order to raise awareness of certain topics among as many people, federal authorities and private companies as possible: a campaign on the use of the OASI number by federal authorities outside the social insurance system (see Focus) and a campaign on tenancy application forms (see Section 1.3).

Data breaches

In the year 2024/25, 344 data breaches were reported via the FDPIC's online form, up significantly from 245 the previous year. The FDPIC received 19 reports via other channels such as email or post. Twenty-six reports were submitted voluntarily.

For this year, the time that elapsed between a data breach occurring and the same being reported to the FDPIC was also calculated: around 40 % of data breaches detected were reported within 6 days, and around 80 % within 21 days.

Table 10: Reporting of data security breaches

Total of reports	363
Submitted voluntarily	26
Within 6 days	40 %
Within 21 days	80 %

Table 9: Supervisory activities and campaigns (see page 22)

Complaints	**1053**
of which	1023 against private entities 30 against federal authorities 788 processed 265 pending
Low-threshold interventions	**108**
of which	**90 % complied with voluntarily**
Preliminary investigations	**20**
Investigations	**9**
of which	6 pending 3 concluded with administrative measures
Pending before the FAC	**2**
Campaigns	**2**
of which	1 for federal authorities 1 for private entities

Information

The proportion of resources used for the Information service group was reduced further during the year under review to 15.1 % from 17.8 % the previous year.

Legislation

The changes in the way personal data is processed with the digital transformation of the federal offices require a large number of new and revised provisions in federal law, on which the FDPIC has expressed his views in various consultation procedures. The workload that this entails for the various FDPIC teams should not be underestimated: Most office consultations involve interdisciplinary analyses in the areas of data protection, IT, international affairs and the Freedom of Information Act. When the projects carry a high residual risk to the privacy or fundamental rights of the data subjects or when large IT projects are proposed, a data protection impact assessment also needs to be carried out, which then has to be reviewed by the FDPIC. During the year under review, the FDPIC took part in 271 office consultations.

Table 11: Office consultations

Total	274
Concluded	250

Services and resources relating to the Freedom of Information Act

The number of staff available for mediation proceedings and recommendations under the Freedom of Information Act remains unchanged at 6 full-time positions. The FDPIC will continue to work towards reducing the processing backlogs caused by the persistently large number of mediation requests. Whether and how quickly this can be achieved will depend on the number and complexity of mediation requests received in the future and the staff resources available.

Table 12: Staff positions available for FoIA issues

2023	5,4
2024	6,2
2025	**6,2**

Participation in committee consultations and parliamentary committee hearings

During the year under review, the FDPIC participated in the following hearings and committee consultations:

- April 2024: LAC-S on the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (e-ID Act);
- April 2024: FC-S and FC-N subcommittees on the financial statement for 2023;
- April 2024: PIC-S on the Federal Act on the National System for the Retrieval of Addresses of Natural Persons (National Address Service Act);
- May 2024: PIC-N on the Federal Act on Data Protection, inclusion of a provision on AI-driven automated decision-making;
- June 2024: PIC-S on the Federal Act on the National System for the Retrieval of Addresses of Natural Persons (National Address Service Act);
- June 2024: CC-S/N subcommittee on the FDPIC's Annual Report 2023/24;
- June 2024: PIC-N on the Passenger Name Records Act (PNRA);
- June 2024: LAC-S on the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (e-ID Act);
- August 2024: SPC-N on the Passenger Name Records Act (PNRA);
- August 2024: PIC-S on the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (e-ID Act);
- August 2024: CC-N office visit by the FDJP/FCh subcommittee;
- October 2024: FC-S and FC-N subcommittees on the 2025 budget;
- October 2024: PIC-N on the Federal Act on the National System for the Retrieval of Addresses of Natural Persons (National Address Service Act);
- October 2024: PIC-N on the Federal Personnel Act (FPA).

Service visit by the FDJP/FCh sub-committee of the National Council Control Committee

Operating under a parliamentary mandate, the control committees (CC) exercise oversight over the conduct of business by the Federal Council and the Federal Administration, the federal courts and other bodies entrusted with tasks of the Confederation.

In that context, the FDJP/FCh sub-committee met with the FDPIC and his senior staff on 27 August 2024 to discuss the mandate, duties and responsibilities of the FDPIC as well as ongoing cases. The visit provided an opportunity to discuss current challenges and to gauge staff satisfaction. The FDPIC also had a chance to present the most important current issues regarding data protection and the principle of transparency.

The FDPIC's data protection officer

The FDPIC's data protection officer (DPO) has the following tasks: responding to requests for information, reviewing the processing of personal data by the FDPIC as an authority, and recommending corrective action if a breach of data protection regulations is identified. The DPO also reviews the application and updating of the provisions on data processing.

During the year under review, the data protection officer received sixteen requests for information and one request for erasure. He provided six data subjects with the requested information within the statutory time frame. The remaining requests concerned personal data that was not available to the FDPIC and that he did not process. These requests had been submitted under the erroneous assumption that the FDPIC had access to all databases and personal data held by the Federal Administration, which is not the case.


17:32
5G
Abbrechen
Fotos
Sammlungen
Fertig
Mediathek durchsuchen ...
Beschränkter Zugriff auf deine Mediathek
„Instagram“ kann nur auf die Objekte zugreifen, die du auswählst. Die App kann Inhalte zu deiner Mediathek hinzufügen, selbst wenn keine Objekte ausgewählt sind.

3.2 Communication

In 2024, the FDPIC published 15 short news reports and five media releases and issued 30 recommendations relating to the Freedom of Information Act, which were published on his website. In terms of case law, the Federal Administrative Court ruled 14 times and the Federal Supreme Court once on the principle of freedom of information within the Administration. Some parts of the Federal Administration are still looking to exclude some or all of the Administration's activities from the scope of application of the Freedom of Information Act. The FDPIC has compiled a list of these, which is available on his website.

Media releases

The FDPIC always issues a media release on conclusion of formal proceedings. In 2024, these were case investigations into the federal offices of fedpol and BAZG within the Administration and the companies Xplain and Digitec Galaxus and the auction platform Ricardo in the private sector. All proceedings were concluded under the old law.

Short news reports

Seven short news reports concerned cross-border data protection. For example, the FDPIC intervened with the Meta Group, which wanted to use the data of users in Switzerland to improve its artificial intelligence without their consent. With growing concerns about mass scraping of personal information on social media platforms, particularly to support AI systems, the FDPIC teamed up with 16 other national data protection authorities to issue a joint concluding statement describing how social media companies could better protect personal information.

Information and awareness-raising

Since the relaunch of his website in 2023, the FDPIC has continued to work on creating a range of useful information and tools, particularly in connection with changes following the entry into force of the fully revised Federal Act on Data Protection but also in view of

the ongoing process of digitalisation and associated technological phenomena such as AI. These include guidelines on data processing using cookies and similar technologies, guidelines on reporting data security breaches and informing data subjects in accordance with Article 24 FADP, a factsheet on FDPIC investigations of violations of data protection regulations, and a factsheet on planning and justifying online access to personal data.

Website

The website has been overhauled again with migration to the new software and offers quick and easy access to assistance in the form of comprehensive FAQs. The new contact forms offer stakeholders a simple, direct way to submit their concerns to the FDPIC. The reporting portals remain a popular tool (see statistics). All guidelines and factsheets can be found in the documentation section.

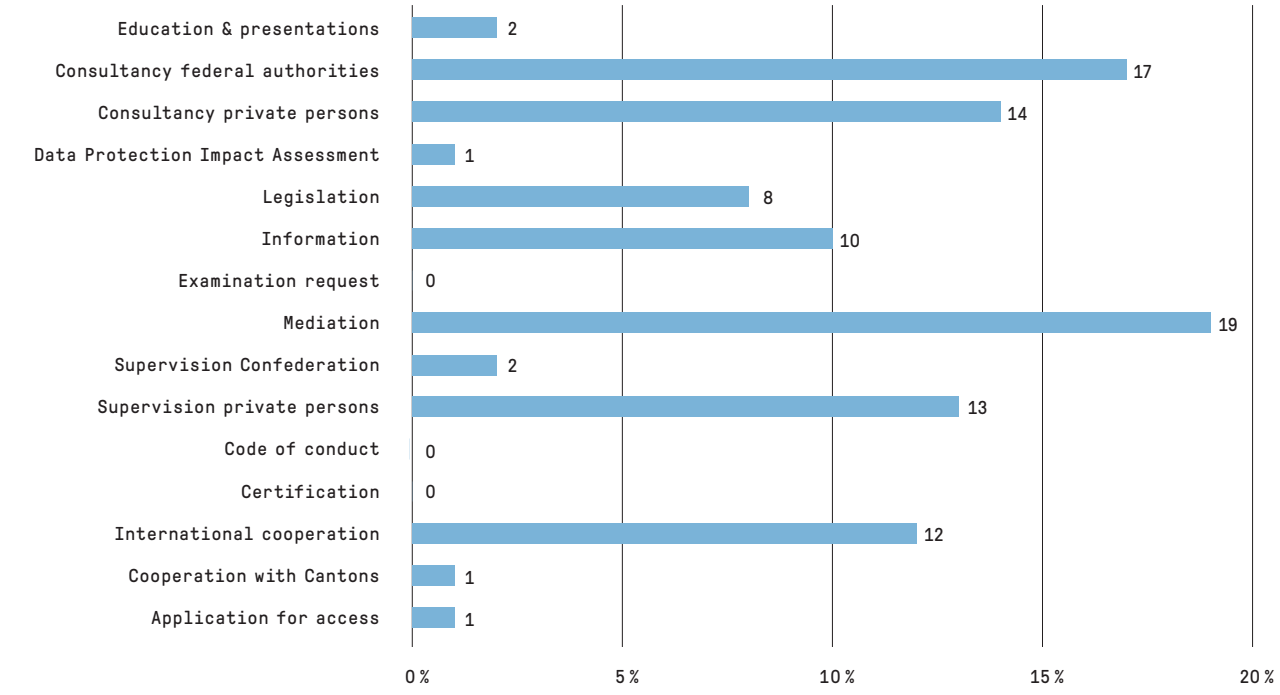
Media relations

The FDPIC answered around 200 media enquiries last year. Reporting on current topics relating to data protection, data security, the Freedom of Information Act and the requirement for transparency within the Administration helps to raise public awareness and is an important part of the FDPIC's communication activities, even if – or particularly if – it causes controversy. For example, the FDPIC regularly voices critical opinions in public on behalf of the citizens concerned.

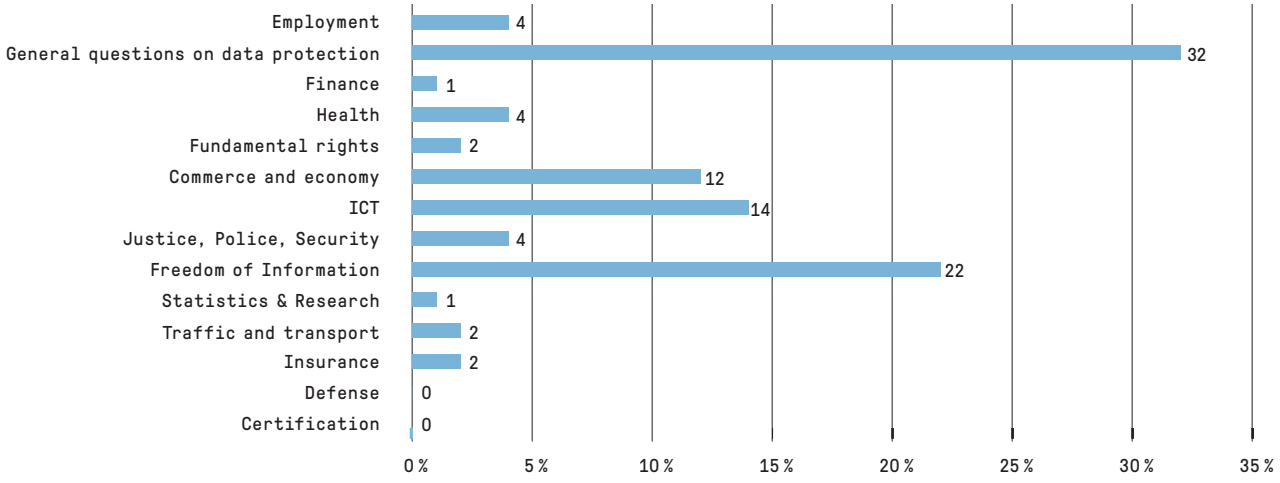
3.3 Statistics

Statistics on FDPIC's activities from 1st April 2024 to 31 March 2025

Workload per tasks in %



Workload per material in %



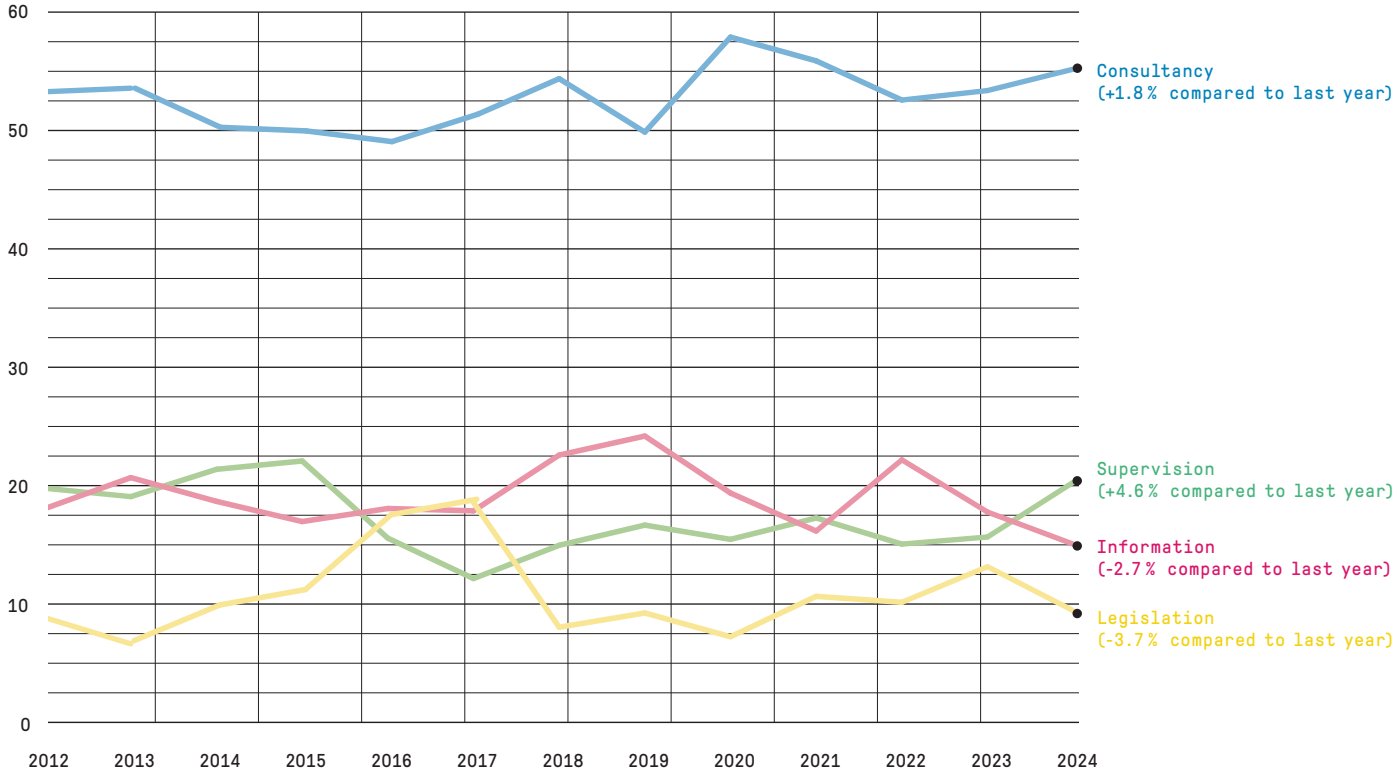
Number of process instances

Mediation proceedings	184
Office consultations	274
Consulting services	1248
Investigations following a report	1087
Complaint procedures	9
Conferences and events	49
Media requests	170
Hotline calls	1180
Requests by contact forms	1823
Requests by email	914
Incoming letters by post	604

Total of receipts from natural persons	**3668**
Total of standard rejections	**584**
Percentage of standard rejections	16 %

Multi-year comparison

(as a percentage)



Overview of applications for access under the Freedom of Information Act from 1st January to 31 December 2024

Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
FCh	123	68	12	30	1	8	4
FDFA	306	137	27	77	6	15	44
FDHA	292	131	17	79	19	25	21
FDPJ	212	111	20	37	10	3	31
DDPS	527	366	23	90	10	8	30
FDF	145	54	28	43	4	5	11
EAER	290	146	25	35	63	13	8
DETEC	324	142	23	82	20	22	35
OAG	8	3	2	0	0	3	0
PS	5	1	2	1	0	0	1
Total 2024 (%)	2232	1159 (52)	179 (8)	474 (21)	133 (6)	102 (5)	185 (8)
Total 2023 (%)	1738 (100)	830 (48)	176 (10)	402 (23)	73 (4)	96 (6)	161 (9)
Total 2022 (%)	1180 (100)	624 (53)	99 (8)	236 (20)	53 (5)	69 (6)	99 (8)
Total 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (4)	78 (6)	115 (8)
Total 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Total 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Total 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Total 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	–
Total 2016 (%)	554 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	–
Total 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	–
Total 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	–

Statistics on applications for access under the Freedom of Information Act from 1st January to 31 December 2024

		Number of requests	that were submitted in previous years	Access completely granted	Access completely denied	Access partially granted//suspended	Request withdrawn	Pending requests	No dcument available
Federal Chancellery FCh	FCh	**94**	0	50	11	26	1	2	4
	FDPIC	**29**	0	18	1	4	0	6	0
	Total	**123**	**0**	**68**	**12**	**30**	**1**	**8**	**4**
Federal Departement of Foreign Affairs FDFA	FDFA	**306**	0	137	27	77	6	15	44
	Total	**306**	**0**	**137**	**27**	**77**	**6**	**15**	**44**
Federal Departement of Home Affairs FDHA	GS FDHA	**22**	0	13	2	4	0	1	2
	FOGE	**8**	1	8	0	0	0	0	0
	FOC	**15**	0	9	2	2	0	2	0
	SFA	**2**	1	2	0	0	0	0	0
	METEO CH	**3**	0	3	0	0	0	0	0
	NL	**0**	0	0	0	0	0	0	0
	FOPH	**85**	0	21	4	41	4	13	2
	FOS	**4**	0	4	0	0	0	0	0
	FSIO	**32**	0	21	0	6	1	0	4
	FSVO	**42**	0	23	2	8	3	3	3
	SNM	**0**	0	0	0	0	0	0	0
	swissmedic	**70**	8	25	5	18	11	3	8
	Suva	**7**	0	2	2	0	0	1	2
	compenswiss	**2**	0	0	0	0	0	2	0
	Total	**292**	**10**	**131**	**17**	**79**	**19**	**25**	**21**
Federal Department of Justice and Police FDJP	GS FDPJ	**34**	1	19	0	6	1	0	8
	FOJ	**54**	2	25	10	4	2	0	13
	fedpol	**35**	0	9	10	11	0	2	3
	METAS	**2**	0	2	0	0	0	0	0
	SEM	**61**	0	39	0	12	6	0	4
	PTSS	**2**	0	1	0	1	0	0	0
	SIR	**4**	0	3	0	0	0	0	1
	IPI	**4**	0	4	0	0	0	0	0
	FGB	**6**	0	4	0	0	1	1	0
	ESchK	**2**	0	2	0	0	0	0	0
	FAOA	**5**	0	2	0	3	0	0	0
	ISC	**3**	0	1	0	0	0	0	2
	NKVF	**0**	0	0	0	0	0	0	0
	Total	**212**	**3**	**111**	**20**	**37**	**10**	**3**	**31**

		Number of requests	that were submitted in previous years	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Federal Department of Defence, Civil Protection and Sport DDPS	GS DDPS	**87**	5	19	7	39	5	5	12
	Defence	**38**	0	9	0	19	3	0	7
	FIS	**16**	0	2	1	10	0	0	3
	OA-IA	**12**	1	2	7	2	1	0	0
	armasuisse	**18**	1	2	4	9	1	2	0
	FOSPO	**317**	0	311	2	0	0	1	3
	FOCP	**8**	0	4	0	4	0	0	0
	swisstopo	**4**	0	3	0	0	0	0	1
	OA	**2**	0	2	0	0	0	0	0
	SEPOS	**23**	0	11	2	7	0	0	3
	NCSC	**2**	0	1	0	0	0	0	1
	Total	**527**	**7**	**366**	**23**	**90**	**10**	**8**	**30**
Federal Departmemt of Finance FDF	GS FDF	**27**	1	9	6	8	1	0	3
	FFA	**11**	0	6	2	2	0	1	0
	FOPER	**5**	0	4	0	1	0	0	0
	FTA	**20**	0	7	3	8	0	1	1
	FOCBS	**32**	5	8	9	10	0	3	2
	FOBL	**12**	0	7	4	1	0	0	0
	FOITT	**4**	0	2	0	1	0	0	1
	SFAO	**18**	0	8	4	3	2	0	1
	SIF	**11**	0	1	0	7	0	0	3
	PUBLICA	**4**	0	1	0	2	1	0	0
	CCO	**1**	0	1	0	0	0	0	0
	Total	**145**	**6**	**54**	**28**	**43**	**4**	**5**	**11**

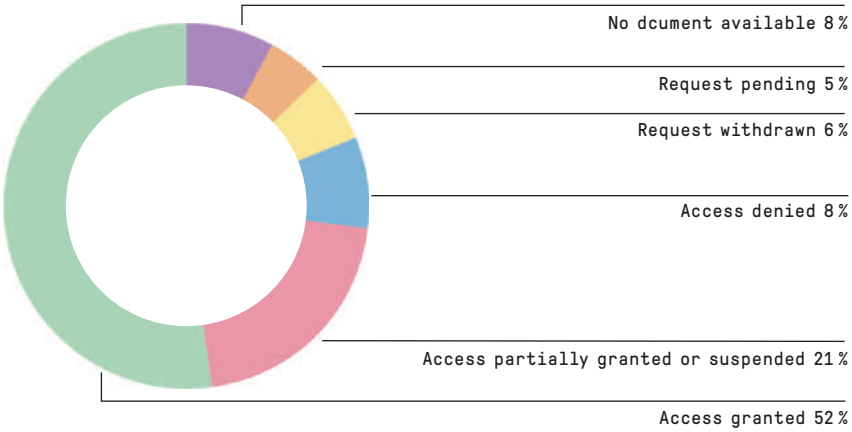
		Number of requests	that were submitted in previous years	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	**20**	0	6	2	4	2	4	2
	SECO	**51**	1	16	10	16	8	1	0
	SERI	**11**	0	6	2	1	0	0	2
	FOAG	**22**	2	12	2	3	2	0	3
	Agroscope	**3**	0	2	0	0	0	1	0
	FONES	**0**	0	0	0	0	0	0	0
	FHO	**4**	0	4	0	0	0	0	0
	PUE	**8**	0	3	1	4	0	0	0
	COMCO	**16**	0	9	1	3	0	2	1
	ZIVI	**3**	0	3	0	0	0	0	0
	FCAB	**1**	0	1	0	0	0	0	0
	SNSF	**4**	1	1	2	1	0	0	0
	SFIVET	**0**	0	0	0	0	0	0	0
	ETH Board	**143**	0	81	5	2	50	5	0
	Innosuisse	**4**	0	2	0	1	1	0	0
	Total	**290**	**4**	**146**	**25**	**35**	**63**	**13**	**8**
Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	**31**	1	13	2	3	0	1	12
	FOT	**19**	0	9	0	5	1	2	2
	FOCA	**26**	2	10	4	6	3	0	3
	SFOE	**19**	1	9	0	6	2	2	0
	FEDRO	**27**	0	23	0	2	1	0	1
	OFCOM	**34**	2	7	2	11	5	3	6
	FOEN	**144**	5	58	14	43	8	11	10
	ARE	**9**	0	8	1	0	0	0	0
	ComCom	**2**	0	1	0	1	0	0	0
	ENSI	**7**	3	2	0	3	0	2	0
	ESTI	1	0	0	0	0	0	1	0
	PostCom	**3**	2	1	0	2	0	0	0
	ICA	**0**	0	0	0	0	0	0	0
	FPI	**0**	0	0	0	0	0	0	0
	SUST	**2**	0	1	0	0	0	0	1
	Total	**324**	**16**	**142**	**23**	**82**	**20**	**22**	**35**

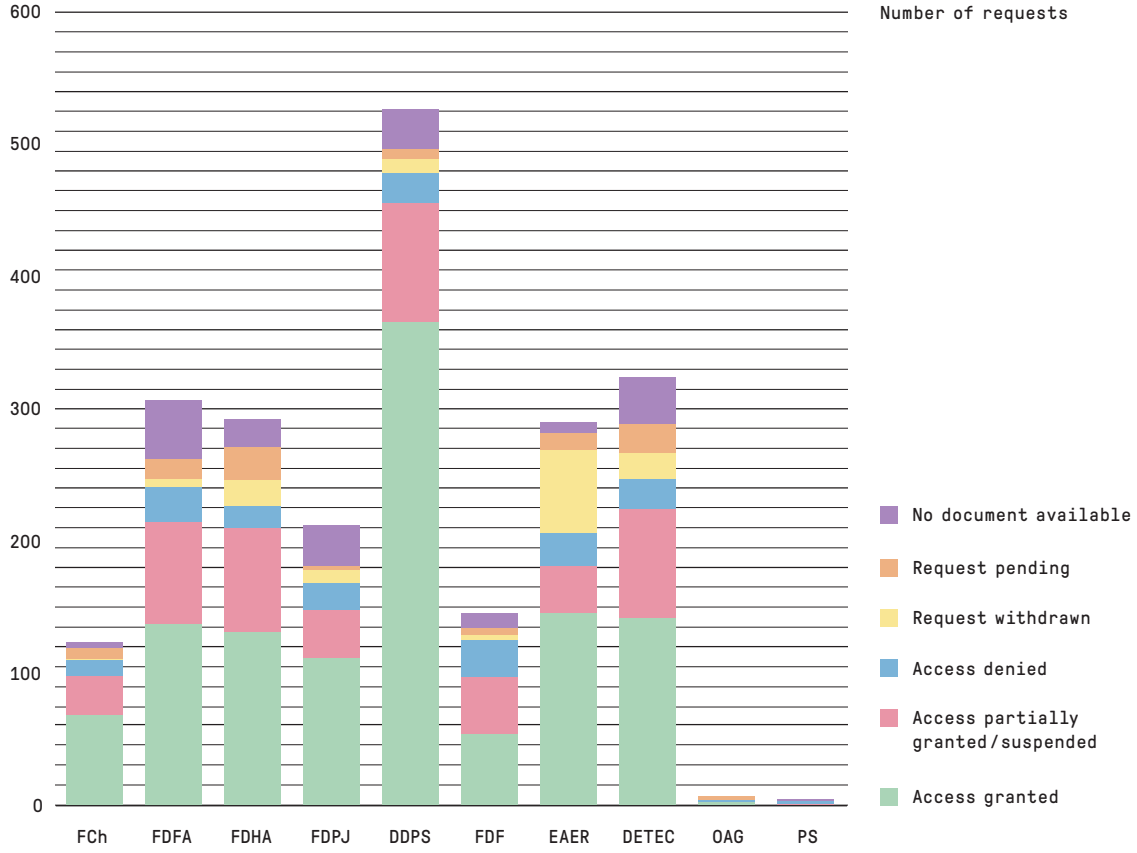
		Number of requests	that were submitted in previous years	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Office of the Attorney General OAG	BA	**8**	0	3	2	0	0	3	0
	Total	**8**	**0**	**3**	**2**	**0**	**0**	**3**	**0**
Parliamentary Services PS	PD	**5**	0	1	2	1	0	0	1
	Total	**5**	**0**	**1**	**2**	**1**	**0**	**0**	**1**
	Total sum	**2232**	**46**	**1159**	**179**	**474**	**133**	**102**	**185**

Number of requests for mediation by applicant category

Applicant category	2024	2023	2022	2021	2020	2019	2018	2017
Media	61	74	47	53	31	34	24	21
Private individuals (or no exact assignment possible)	66	31	37	49	42	40	26	35
Stakeholders (associations, organisations, clubs etc.)	16	8	9	16	5	7	9	14
Lawyers (for third parties or on their own account)	45	16	27	12	7	5	4	2
Companies	14	3	9	19	7	47	13	7
Universities	0	0	0	0	1	0	0	0
Total	**202**	**132**	**129**	**149**	**93**	**133**	**76**	**79**

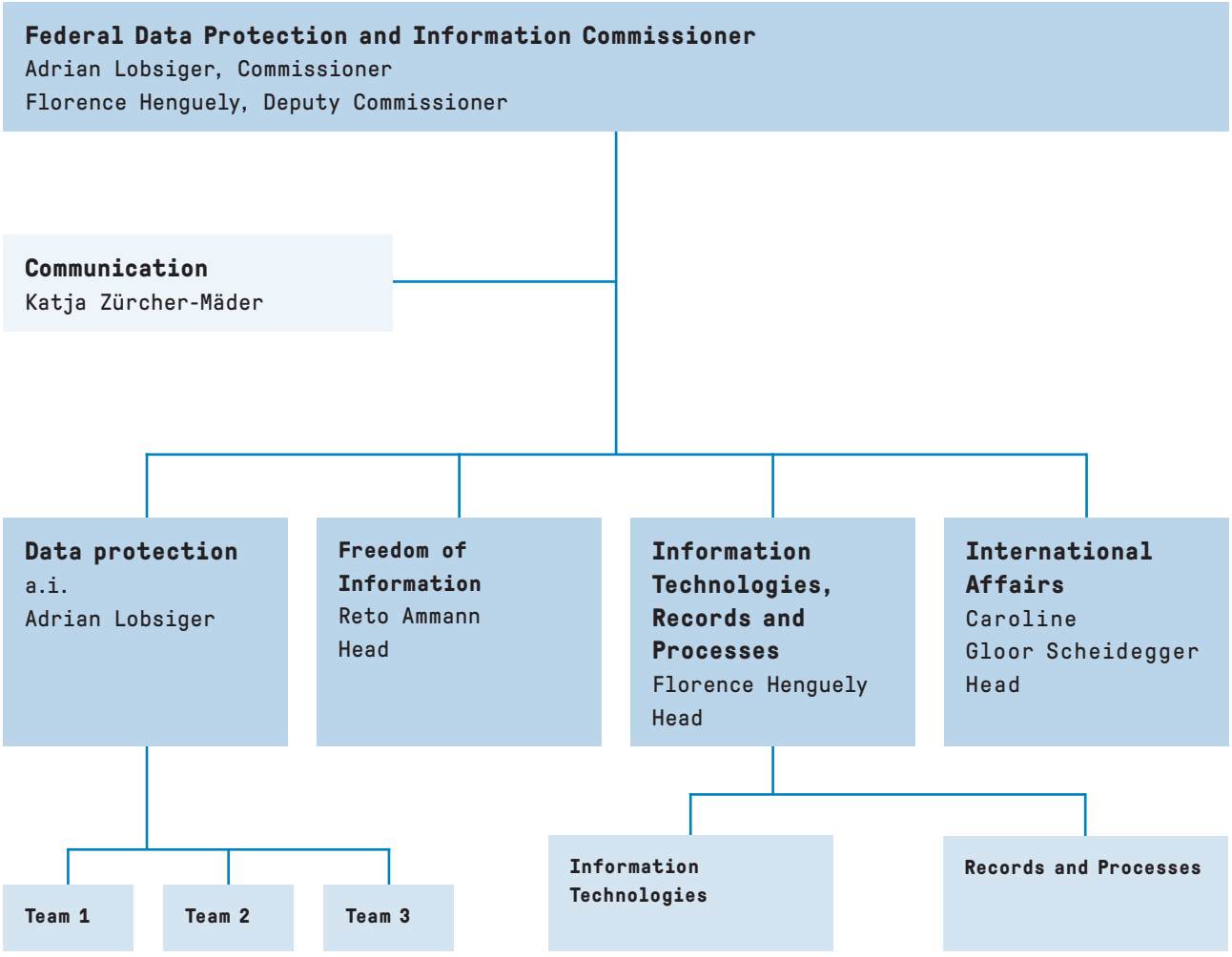
Applications for access in the federal administration from 1st January to 31 December 2024





3.4 Organisation FDPIC (Status 31 March 2025)

Organisation chart



Employees of the FDPIC

Number of employees	44		
FTE	37.2		
per gender	Women	22	50 %
	Men	22	50 %
by employment level	1–89 %	29	65.91 %
	90–100 %	15	34.09 %
by language	German	31	70.45 %
	French	12	27.27 %
	Italian	1	2.27 %
by age	20–49 years	25	56.82 %
	50–65 years	19	43.18 %
Management	Women	5	55.56 %
	Men	4	44.44 %
	Total	9	

Abbreviations

AI Artificial intelligence

CDEP Committee on Digital Economy Policy of the OECD

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

DPO Ordinance to the Federal Act on Data Protection

DPSS Digital Public Services Switzerland

DTI Digital Transformation and ICT Steering Sector of the Federal Chancellery

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

E-ID Electronic Identity

EPR Electronic Patient Record

EPRA Electronic Patient Record Act

FADP Federal Act on Data Protection

FAOA Federal Audit Office Act

FDPIC Federal Data Protection and Information Commissioner

Fedpol Federal Office of Police

FIS Federal Intelligence Service

FOCBS Federal Office for Customs and Border Security

FoIA Freedom of Information Act

FoIO Ordinance on Freedom of Information in the Administration

GDPR General Data Protection Regulation

GPA Global Privacy Assembly

ICT Information and Communication Technology

IntelSA Federal Act on the Intelligence Service

NCSC National Cyber Security Centre

PNR Passenger Name Records

PNRA Passenger Name Records Act

Privatim Association of Swiss Commissioners for Data Protection

SAS Swiss Accreditation Service

VIS Visa Information System

Figures and tables

Figures

Tables

Impressum

This report is available in four languages and also in an electronic version on the Internet.
Distribution: BBL, Verkauf Bundespublikationen, CH-3003 Bern
www.bundespublikationen.admin.ch
Art.-Nr. 410.032.ENG

Layout: Ast & Fischer AG, Wabern
Photography: Monika Flückiger
Caracters: Pressura, Documenta
Print: Ast & Fischer AG, Wabern
Paper: PlanoArt®, woodfree bright white

Key figures

Workload data protection

55.1 %	20.3 %	15.1 %	9.5 %
Consultancy	Supervision	Information	Legislation

Supervision

108	19	9	2
Low-threshold interventions	Preliminary enquiries	Formal investigations Art. 49 FADP	pending before FAC

Applications for access to the FDPIC

18	4	1	0	6	0
granted	partially granted or suspended	denied	withdrawn	pending	no document available

Federal Data Protection and Information Commissioner
Feldeggweg 1
CH-3003 Bern

E-Mail: info@edoeb.admin.ch
Website: www.thecommissioner.ch
@EDÖB – PFPDT – IFPDT
Phone: +41 (0)58 462 43 95 (Mo – Fr, 10 – 11:30 am)
Fax: +41 (0)58 465 99 96