

31th Annual Report 2023/24

Federal Data Protection and
Information Commissioner



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Annual Report 2023/2024

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 2023 and 31 March 2024 for the section on data protection. For the section on freedom of information it corresponds to the calendar year 1 January to 31 December 2023.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Foreword

After the new Federal Act on Data Protection came into force on 1 September 2023, our authority continued to publish fact sheets and interpretive guidance for businesses, authorities and members of the public. Our work on the transition from the old law to the new one will soon be complete, and the additional posts allocated by Parliament will be assigned primarily to conducting investigations.

However important the legislative changes introduced by the new Federal Act on Data Protection are from a practical point of view, it is important to remember that privacy-friendly processing of personal data requires a basic understanding of the fundamentals of privacy. Therefore, in this edition of the Annual Report, I would like to shed light on some key aspects by answering seven questions that I was frequently asked during my first two terms of office.

Adrian Lobsiger
Federal Data Protection and Information Commissioner



Bern, 31 March 2024

Current Challenges 6**Data protection****1.1 Digitalisation and fundamental rights . 14**

- Federal Cloud Strategy: CEBA project of the Federal Chancellery
- Digital transformation of the healthcare system: Personal identifier
- Legislation on communicable human diseases: Use of the OASI number
- Digital identity: FDPIC actively involved in finalising the e-ID bill
- Legislation: Implementation of the Information Security Act

Focus 20

The new Data Protection Act

1.2 Justice, Police, Security 26

- Investigation against fedpol, FOCBS and Xplain: RIPOL access and data breach
- Cyber attack: Preliminary investigations regarding Concevis
- Police database: The FDPIC calls for compliance with data protection rules in the digitalisation of police administrative assistance

1.3 Economy and society 31

- Online campaign to gauge priests' core beliefs: Investigation into the 'Bürgerforum Schweiz'
- Tenancy application form: Preliminary investigation at a property management company
- Auction platform Ricardo: Final report including recommendations
- Customer data: Investigation into Digitec Galaxus
- Dating app: Case investigation concluded at Once Dating AG
- Tracking technologies: Concerns over Oracle America allayed: Swiss residents unaffected by controversial data processing
- Transparency of legal entities: Introduction of a register of beneficial owners
- Economy: New legislation to screen foreign investments

1.4 Health 38

- Supervision of the health insurance industry: Exchanges between the FDPIC and the FOPH
- Vaccination data: Project to recover data from the meineimpfungen.ch platform
- Medical practice: Patients required to sign a new consent form

- Data reuse: The Federal Act on Data Protection versus the Federal Act on Research Involving Human Beings
- Electronic patient record: Comprehensive revision of the Federal Act on the Electronic Patient Record

1.5 Employment 44

- Employment law: Personnel record-keeping requirements
- Employment law: Data protection rules applicable to pension funds

1.6 Transport 46

- Numerous projects: Consultancy and office consultations on mobility
- PNR data: Office consultation on the Passenger Name Records Act

1.7 International 49

- European Union: EU adequacy decision
- Data Privacy Framework (DPF): Framework for data transfers to the US
- Council of Europe: Convention 108+ has been ratified
- Europe: Meeting with ICO and EDPB
- European Case Handling Workshop: International meeting in Switzerland
- Joint statement: Joint statement on data scraping and data protection
- International: OECD
- Schengen: BTLE and EDPB
- Schengen: Supervision Coordination Groups on the SIS II, VIS and Eurodac information systems
- Schengen: Schengen Coordination Group of the Swiss data protection authorities
- Schengen: Schengen-related activities at national level
- International meeting: Association of Francophone Data Protection Authorities
- International cooperation: Privacy Symposium in Venice
- Global issues: Global Privacy Assembly
- International: European Conference of Data Protection Commissioners in Budapest

Freedom of Information

2.1 General	62
2.2 Applications for access: sharp rise in 2023	64
2.3 Mediation procedures: slight increase in mediation requests	68
– Proportion of amicable outcomes	
– Duration of mediation procedures	
– Number of pending cases	
2.4 Legislative process	72
– Finance: Credit Suisse: Emergency ordinance incorporated into the Banking Act	
– Archiving: Partial revision of the Archiving Ordinance	
– Financial crime: New federal act on the transparency of legal entities	
– Fees: Free of charge as a principle: fees charged only for applications that take particularly extensive processing	
– CC-S report: Opinion of the Federal Council	
2.5 Special reservations under Art. 4 FoIA	78

The FDPIC

3.1 Duties and resources	82
– Services and resources in the field of data protection	
– Services and resources in the field of freedom of information	
– DPO and ITSO: FDPIC improves self-regulation	
3.2 Communication	86
– New website with reporting portals	
– Figures	
– Issues	
3.3 Statistics	88
– Statistics on FDPIC's activities from 1 st April 2023 to 31 March 2024 (Data protection)	
– Overview of applications for access under the Freedom of Information Act from 1 st January to 31 December 2023	
– Statistics on applications for access under the Freedom of Information Act from 1 st January to 31 December 2023	
– Requests for access 2023 with Corona reference	
– Number of requests for mediation by applicant category	
– Applications for access in the federal administration from 1 st January to 31 December 2023	
3.4 Organisation FDPIC	98
– Organisation chart	
– Employees of the FDPIC	
Abbreviations	100
Figures and tables	101
Impressum	102
In the cover	
– Key figures	
– Data protection concerns	

Current Challenges

I Data protection

In view of the dynamics of digitalisation, the public debate has become somewhat fixated on technological phenomena, for whose assessment under data protection law technological knowledge may be useful, but without a basic understanding of the peculiarities of data protection, it usually proves to be insufficient. Against this backdrop it seems helpful to us to answer seven frequently asked questions about data protection:

1. What data is protected under data protection law?

Data protection protects the personality and fundamental rights of natural persons by regulating the processing of personal data and protecting the data subjects from processing by which the state interferes with their fundamental rights or private companies interfere with their privacy and self-determined lifestyle.

Data protection is therefore not directly aimed at the «protection of data», as the latter cannot be the bearer of rights. It also does not protect data ownership or exclusive rights to data like intellectual property law. Information held by private individuals under commercial and manufacturing secrecy or police and military secrets

of the state are also generally not relevant to data protection because the interest in keeping them secret typically relates to the factual content of the information, such as a brewing recipe or weapons technology.

2. What is an individual's 'personality' and what is it being protected from?

The human personality as the very nucleus of data protection is what children refer to as 'I' soon after they learn to say their own name. Legally defining the individual's 'I' is a challenge. Although the Federal Constitution, the Civil Code and the Federal Act on Data Protection state that the individual's personality is legally protected, they do not define the term *per se*. However, according to legal theory and case law, 'personality' refers to a person's individual characteristics – their innermost nature – which characterise them as an individual while at the same time distinguishing them from other people.

3. Where do private and intimate spheres begin and how far do they extend?

An individual's 'I' is defined by their body, face, voice and behaviour. From a medical point of view, an individual's 'I' is situated in internal organs such as the brain. From there, the core of an individual's intimacy and privacy extends to the outer body and the space inhabited by that individual. In that core area, data protection prevents or hinders intrusive means of data collection such as lie detectors or neural implants. Also devices such as camera-equipped drones, telephoto lenses and sensors that observe people's behaviour in this area are also prohibited in principle.

In their digitalised everyday lives as consumers, passers-by, passengers or patients, people create and leave behind a trail of electronic information that could technically be used to draw conclusions about their personality. As a result, an individual's intimacy and privacy – and therefore data protection – extends from their body and home to their smartphone and on to the cloud, where the private operators of data centres process vast amounts of text and voice messages, images and meta-data such as websites visited or phone calls held. Data protection law sets

«The human personality is the very nucleus of data protection.»

limits on the processing and linking of data also in this extended area of privacy and intimacy.

4. Can consenting adults waive their data protection rights?

The protection of privacy is a constitutionally guaranteed fundamental right (Art. 13 of the Federal Constitution). In principle, there is no voluntary waiver of data protection rights with regard to the processing of personal data by the State. The purpose, scope and extent of data processing by the State are determined by statutory provisions that are binding for the authorities and from which they cannot be legally released in specific cases.

However, data subjects may consent to private processing of personal data that violates their privacy. That said, their waiver is only effective under data protection law if they have been fully and adequately informed in advance and their waiver is genuinely voluntary. Whether or not consent to specific data processing can be considered voluntary depends on the individual's circumstances, for example the

financial means of users of digital services: Not all users can afford to forgo the high discounts offered by private providers of goods and services in exchange for disclosing personal information as part of digital customer programmes. Furthermore, when individuals apply for employment, insurance or a rental property, high demand may not be used as a pretext for an excessive invasion of privacy by requiring applicants to provide supposedly voluntary information about their private lives. Consent given in such circumstances may prove invalid under data protection law.

5. Is privacy an outdated concept in the digital age with more and more people sharing everything about themselves on social media?

Millions of people document their lives on a daily basis with text, images and voice messages, sharing the information online with friends or paying customers or even making it accessible to the general public. However, adults seen presenting themselves in seemingly spontaneous poses for a wide audience are usually keen to portray themselves and their lives in a carefully staged manner. The vast majority of them are vulnerable and vigorously opposed to information about their actual private lives being obtained and disseminated without their consent.

Therefore, we see a growing need – rather than a decreasing one – for data protection in order to ensure that social network operators comply with their terms of use and do not process personal data that users do not share or only share selectively for their own purposes, including disclose it to third parties.

6. Are there any forms of data processing that are prohibited?

When regulating the processing of personal data by the authorities, lawmakers are obliged to respect the fundamental right to privacy and informational self-determination, with which the Federal Constitution guarantees individuals the right to lead private and self-determined lives. Any laws that were to introduce data processing activities by the State that undermined fundamental rights such as freedom of political expression and participation would be in conflict with the Constitution.

Unfortunately, the requirements of the Constitution and democracy are not always understood by the promoters of government digitalisation projects. When supervising such projects, the data protection authorities must

always insist that the power-limiting mechanisms of democracy – e.g. the separation of powers, federalism or the division of administrative power among specialist authorities – not be discarded as ‘outdated practices’ but rather be included in data flow automation.

The situation is different for the processing of personal data by private entities. In principle, this is permitted in Switzerland. Data protection law – which is based on principles – only provides a general, abstract answer as to when the invasion of an individual’s privacy reaches a level that cannot be justified by consent or overriding interests.

Data protection law takes a graduated approach to setting a limit for what is permissible, whereby legally binding consent to the collection of personal data can be declared invalid when data collection exceeds what is necessary for achieving the intended purpose by exploiting ignorance or a relationship of dependence.

An absolute limit is reached when an individual’s consent would deprive them of their freedom or restrict their freedom to a degree that violated morality or the law as a whole, as set out in the Civil Code.

7. How political is data protection?

Historically, the concept of data protection itself has its roots in the political model of liberalism.

In liberal constitutional states such as Switzerland, the protection of data and privacy entitles individuals to lead a private and self-determined life that goes beyond a mere right to exist. On the one hand, this principle sets liberal

societies apart from totalitarian models of government and society, in which the individual is placed under collective rule; on the other hand, a model of society that is geared towards the right to enjoy life through self-fulfilment is in contrast with the efficient forms of organisation of other life forms such as insects or lifeless technology such as artificial intelligence.

Freedom would be totally eroded and privacy would become a thing of the past, for example, in a state or economic social order in which people became the mere object of collective goals in terms of absolute health, economic and police security and perhaps even absolute ecological sustainability through total monitoring and permanent self-measurement.

Irrespective of this historical derivation of data protection, data protection authorities fulfil their statutory duties in a democratic constitutional state in an apolitical manner.

«Mature adults who supposedly pose freely for a wide audience, usually attach importance to present themselves in a in a self-staged context.»

II Current challenges to freedom of information

Processing time for information requests and mediation procedures

The growing interest in freedom of information has led to an increase in the number of requests for access to documents of the Administration. This has sometimes impacted processing time, resulting in longer waits for applicants. Although the Freedom of Information Act (FoIA) sets clear legal requirements for the individual steps of the procedure, in practice, deadlines are not always met.

The same applies to mediation procedures: 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 procedures (see Section 2.3). Extensive requests – often involving email correspondence over extended periods of time – and complex legal issues typically result in longer procedures. For example, ques-

tions regarding the application of the FoIA 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 increasing and the number of requests for access to documents of the Administration set to continue growing, completing mediation procedures within the required time frame is likely to remain a challenge.

Growing number of special statutory exemptions to the FoIA

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 of this sort 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 on a case-by-case basis by interpreting the relevant rules.

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

III National and international cooperation

International

In a long-awaited decision, the European Commission confirmed in mid-January 2024 that Switzerland offers an adequate level of data protection. This means that personal data can continue to flow freely from a Member State of the European Union (EU) or the European Economic Area (EEA) to Switzerland without the need for additional safeguards to ensure an adequate level of data protection. This is of great economic importance to companies in Switzerland, the EU and the EEA.

During the past financial year, the FDPIC's experts were again actively involved in relevant working groups at an international level, during which

they were able to exchange views face to face with their foreign counterparts. The FDPIC also hosted the annual European Case Handling Workshop in Bern at the beginning of November, where 80 representatives of 37 data protection authorities came together to share their practical expertise.

The FDPIC attended the regular meetings of the data protection bodies of the Council of Europe (Consultative Committee of Convention 108) and the OECD (Working Party on Data

Governance and Privacy in the Digital Economy), the two data protection conferences – European and international – and the conference of the French-Speaking Association of Data Protection Authorities. He also attended the privately organised Privacy Symposium, which dedicated a day to the Council of Europe's modernised convention for the protection of personal data. As the cross-border transfer of personal data continues to raise sensitive legal issues around the world, it is important for data protection authorities to be able to exchange information directly with one another. A number of authorities have signed non-legally-binding Memoranda of Understanding (MoU) in which they pledge to strengthen cooperation.

Cooperation with the cantons

The federal and cantonal data protection authorities have intensified their cooperation in order to ensure effective and comprehensive supervision (see 30th Annual Report, Section III). During the year under review, the FDPIC exchanged views with his cantonal counterparts on a plan which the federal and cantonal administrations are equally keen to pursue, namely to

outsource personal data to data centres operated by the private company Microsoft.

Other issues discussed include the delimitation of competences, and federal versus cantonal jurisdiction in data protection matters. The following scenarios in particular required a more detailed legal analysis: the employment of private data processors by cantonal and communal public bodies; cases in which private or public organisations act both under private law and in a sovereign capacity; and cases in which cantonal law declares the Federal Act on Data Protection to be the applicable data protection legislation.

Data protection

1.1 Digitalisation and fundamental rights

FEDERAL CLOUD STRATEGY

CEBA project of the Federal Chancellery

During the year under review, the FDPIC continued to monitor cloud projects within the Federal Administration closely. In addition to various office consultations, his focus was again on the DTI CEBA (cloud enabling office automation) project.

The CEBA project was classified as a key federal ICT project in 2022 owing to its significant impact on the working methods of virtually the entire Federal Administration. The Digital Transformation and ICT Steering Sector (DTI) of the Federal Chancellery involved the FDPIC in the introduction of the Microsoft cloud-based office application Microsoft 365, and in April 2023 the FDPIC gave his opinion on the guidelines submitted to him on the use of Microsoft 365 and on the draft data protection impact assessment (DPIA) drawn up at his request. He again demanded that all risks be listed transparently in the DPIA, including potential risks that may only emerge at a later date as a result of de facto dependency on the provider with increasing reliance on cloud services.

In the FDPIC's view, it is important for the CEBA project to also study alternatives to the Microsoft 365 cloud solution. The FDPIC has analysed the DTI's activities in this area in detail and has engaged in dialogue with the project team, calling for a broad, unbiased and open-minded approach to the issue. It is important that those responsible in the federal offices have the full facts at their disposal in order to make an informed choice from a range of options (see our statement of 7 March 2023 and the Federal Council's press release of 15 February 2023).

Audit by the SFAO

Having been classified as a key ICT project, the CEBA project was audited by the Swiss Federal Audit Office (SFAO), which also consulted the FDPIC. The purpose of the audit was to establish whether the project was adequately structured and whether the necessary management



and control mechanisms were in place and functioning. The SFAO found that the project had not taken sufficient account of the FDPIC's comments at the time of the audit and recommended that the DTI coordinates more closely with the FDPIC the approach that it chose for the project in terms of data and information protection.

Cloud principles

In connection with the Federal Cloud Strategy, the DTI submitted its fully revised Cloud Principles to the FDPIC in an office consultation. These complement the strategic principles, providing further guidance for implementation of the cloud strategy. The FDPIC was critical of some of the changes introduced in the revised version, particularly as they weakened the binding nature of the principles laid down to the point that these risked no longer being regarded as minimum standards but merely as information and recommendations.

Again in connection with the implementation of the cloud strategy, the FDPIC also took part in an office consultation on the Swiss Government Cloud (SGC), where he expressed his views on the discussion document and the Federal Council decision of the Federal Office of Information Technology and

Telecommunications (FOITT). There, the FOITT proposes that the Federal Council replace the Atlantica private cloud infrastructure that it currently operates with a three-tier hybrid multi-cloud infrastructure: Tier I would include the public cloud services provided by the FOITT via public cloud providers; Tier II would include the solutions of large public cloud providers operated on federal premises; and Tier III would include the FOITT's private cloud, operated entirely via the federal government's own data centre network. The FOITT adopted our proposed amendments and modified various points that have an impact on data protection.

The FDPIC emphasises the importance of addressing data protection issues at a very early stage of projects that involve data processing. In accordance with his mandate, he will continue to oversee the cloud initiatives in an advisory capacity and will monitor compliance with the established criteria and requirements.



Personal identifier

Within the context of the programme to promote the digital transformation of the healthcare system, the FDPIC commented on the work carried out by the expert group for healthcare data management aimed at facilitating the reuse of data by researchers. In particular, he pointed out the data protection aspects that need to be taken into account when developing a personal identifier.

The Federal Department of Home Affairs (FDHA) has launched the DigiSanté programme aimed at promoting the digital transformation of the healthcare system. Many projects involve the use of health data. With regard to the use of data for planning, management and research, the Federal Council has tasked the FDHA with setting up a team of experts to manage healthcare data (GGDS). The Federal Council also discussed creating conditions for the reuse of healthcare data by research institutions, with particular regard to the form of consent given by data subjects for their data to be used and the implementation of a comprehensive data protection strategy to ensure data protection and security.

In connection with the work on the personal identifier, the FDPIC recalled the talks held during the drafting of the provisions on the systematic use of the OASI number outside the field of social insurance, implemented with the introduction of provisions on periodic risk analyses (Art. 153e Federal Act on Old-Age and Survivors Insurance, OASIA) and the implementation of special technical and organisational measures (Art. 153d OASIA).

During the discussions within the working group, the FDPIC also pointed out that the process of creating a personal identifier needed to include not only an assessment of the feasibility and technical aspects but also privacy by design and by default in accordance with Article 7 FADP as well as a data protection impact assessment in accordance with Article 22 FADP for new projects and any planned changes.

Use of the OASI number

The Federal Act on Controlling Communicable Human Diseases and the associated implementing ordinances are currently being revised. From a data protection perspective, one of the main new features is the inclusion of the patient's OASI number among the data that needs to be communicated when a case is reported.

During the year under review, the FDPIC was asked to give his opinion on the draft revisions of the ordinances implementing the Act on Controlling Communicable Human Diseases (EpidA). This legislation requires doctors, laboratories and other health institutions to notify the cantons and the Federal Office of Public Health (FOPH) when they diagnose certain diseases in order to prevent epidemics or help combat them more effectively. From a data protection perspective, one of the main changes introduced with these revisions is the inclusion of the patient's OASI number among the data that needs to be sent when a case is reported. According to the FOPH, using a number that is unique to each individual makes it easier to process case reports and prevent duplication.

Using the OASI number is certainly a means of achieving the goals set by the FOPH. However, the OASI number is a relatively sensitive piece of information as it is used for a wide range of

DIGITAL IDENTITY

activities. If it were to be compromised, this could have quite serious consequences for the data subject. For this reason, the OASI Act (OASIA) stipulates that the use of this number outside the OASI context is subject to enhanced security measures (Art. 153d OASIA). In addition, institutions that use it are required to conduct regular risk assessments (Art. 153e OASIA), independently of the risk assessments required under Article 22 FADP. In his comments, the FDPIC drew particular attention to these points.

Finally, it should be noted that the EpidA is also currently being revised. The FDPIC also commented on this bill. However, the reporting procedure did not yet provide for use of the OASI number, which was only introduced later in the subsequent draft revisions of the ordinances. Nevertheless, the FDPIC and other offices would like to see its use enshrined in formal law. The FOPH has amended the legislation accordingly.

FDPIC actively involved in finalising the e-ID bill

The FDPIC has accompanied the work on the new draft legislation for the e-ID, which provides for a state solution and pursues the self-sovereign approach, from the outset from a supervisory perspective.

After the first bill on a digital identity (e-ID) was rejected in 2021, the Federal Department of Justice and Police (FDJP) drafted a new bill and submitted it for consultation. The FDPIC shared his concerns during a first office consultation (see 29th and 30th Annual Report, Section 1.1). During the year under review, the Federal Office of Justice held two further consultations on the Act before the bill and the associated dispatch were published on 22 November 2023.

The bill regulates both the State-issued digital identity (e-ID) and the operation of a technical infrastructure allowing a wide range of electronic credentials to be issued and verified. This infrastructure can be used by cantonal and communal authorities as well as by private-sector actors wishing to issue and/or use documents such as diplomas, concert tickets or extracts from the register of criminal convictions. The e-ID will be a form of electronic identification issued by the federal office of police (fedpol) at the user's request, enabling users to identify themselves digitally in a secure, fast and uncomplicated way.



Citizens will use an application provided by the State that will act as an electronic wallet, in which they will be able to store and manage their

electronic credentials. The data will be stored locally on their smartphones, and the app will allow users to control the data that they share with the authorities (for example when requesting a criminal record certificate) or with private actors (for example to prove their age when buying alcohol). Users will thus have control over their data (self-sovereign identity) – which will be stored in a decentralised manner – and only the information that is strictly necessary for a given purpose will be shared (principle of data minimisation). The system will need to be designed in accordance with the principle of privacy by design and by default, meaning that data protection will be guaranteed by the system itself.

In June 2023, the FDPIC commented on the revised bill and dispatch following the consultation that had taken place in 2022. In particular, following his concern that creation of the e-ID could lead to improper ID requests in the digital world, he welcomed the introduction of due diligence to limit the e-ID information that can be requested by verifiers, along with penalties to prevent improper online ID requests. However, he insisted that the dispatch include examples of legitimate and improper requests to illustrate the types of scenarios in which verifiers might request personal data stored in the e-ID. The information provided makes it easier to picture scenarios in which access to personal information stored in the e-ID might be requested within



the context of due diligence: A request for e-ID information from a person who has requested access in accordance with Article 25 FADP would be considered legitimate, whereas a request for a customer's e-ID information for a simple online purchase would be considered improper. If someone needs to verify that an individual is over 18, there is no need for disclosure of their identity or date of birth, but just a simple acknowledgement that they are over 18.

The FDPIC stressed how important it was to prevent improper use of the infrastructure and recommended that the Act should provide for the publication of cases of improper use or well-founded suspicions of improper use of the trust infrastructure. He therefore welcomed the introduction of a trust register, integrated in the infrastructure, designed to guarantee the reliability of issuers and verifiers. He also wanted to see certain revocation obligations applied to all issuers of electronic credentials (not just to fedpol, issuer of the e-ID), obliging them to guarantee data accuracy. The dispatch has been amended accordingly to specify an obligation under the FADP to remove any information in the electronic credentials that is incorrect.

The FDPIC took the opportunity to raise the issue of the use of meta data generated when the base register is

LEGISLATION

consulted, which, in his view, should only be used for the purposes of IT security or technical maintenance of the electronic infrastructure or to trace access to the register. He also stressed that it was important to consider regulating the processing of this meta data and repeated his call for regulation in September 2023 in another office consultation on the dispatch on the e-ID Act and on the outcome of the consultation procedure. This recommendation was adopted.

Overall, the FDPIC is pleased that he was actively involved in this important project from the outset and that many of his concerns have been addressed in the final bill and the corresponding dispatch. However, he regrets the fact that the dispatch does not provide information on the outcome of the risk assessment or of the data protection impact assessment, as stipulated in letter 4.1 of the Federal Council's directives of 28 June 2023 on a prior risk assessment and data protection impact assessment for the processing of personal data by the Federal Administration, which set out the obligations of federal bodies in accordance with Article 22 of the Federal Act on Data Protection.

At the request of the Legal Affairs Committees of both councils, the FDPIC took part in their deliberations on the bill between January and April 2024. If Parliament approves, he will continue to oversee the rollout of the e-ID and the trust infrastructure and provide input, for example in office consultations on the Federal Council's ordinances, in order to guarantee privacy by design and by default.

Implementation of the Information Security Act

[The ordinances implementing the Act on Information Security in the Confederation came into force on 1 January 2024. The DDPS has taken into account many of the comments made by the FDPIC during the various consultations.](#)

Parliament adopted the Information Security Act (ISA) at the end of 2020. In the implementation of the act, several ordinances were amended, namely the information security ordinance, the ordinance on personnel security screening, the ordinance on security screening for businesses and the ordinance on federal identity management systems and directory services. During the

various office consultations, the FDPIC made several comments and raised a number of questions. On the subject of personnel security screening, he noted that the formal legal framework of the ISA did not cover all the sensitive data processed under the ordinance. The legal basis will be completed when the act is next revised. The FDPIC also called for clarification in the information security ordinance. It states that the administrative authorities responsible for operational security need to monitor the use of their IT infrastructure and examine it regularly for threats and technical vulnerabilities. The FDPIC suggested amending the provision by specifying that use of the IT infrastructure needed to be monitored by appropriate technical and organisational means and that a regular inspection needed to be automated.

The DDPS rejected the FDPIC's proposal and the difference remained after the last office consultation. The Federal Council also ignored his views, and the ISA implementing ordinances came into force on 1 January 2024.

The new Data Protection Act

Revised Data Protection Act in force

The new Federal Act on Data Protection and the associated ordinances came into force on 1 September 2023. The FDPIC held a number of information events, created guides and fact sheets, and reorganised his website.

In the run-up to the entry into force of the new Federal Act on Data Protection, the FDPIC focused on raising public awareness and informing experts in the private sector and in the Federal Administration.

Information events

During the course of the year, the FDPIC was invited to present the new Act at various information events organised by federal offices and departments. In August, he held a one-day information event at the University of Fribourg for all data protection officers working for the federal bodies. The event was attended by more than 80 participants from a number of different administrative units, who exchanged views on various practical aspects of data protection such as data protection impact assessments, the logging of automated processing operations, and the new rules of procedure.

The FDPIC also answered practical questions from the private sector on the transition to the new FADP at a number of events. He focused specifically on events attended by company data protection officers, covering the different language regions. In the German-speaking part of Switzerland, he attended the autumn event of the Data Privacy Community and university events as well as the regular meetings with the Association for Corporate Data Protection (VUD). In Lausanne, the FDPIC addressed the Swiss Association of Data Protection Officers (ASDPO) as well as the masterclass for aspiring data protection officers. The Data Protection Authority of the Principality of Liechtenstein invited him to present the new Swiss legislation to the data protection officers of Liechtenstein-based companies. The Fédération des Entreprises Romandes (federation of companies in the

French-speaking part of Switzerland) invited him to discuss the practical aspects of data protection directly with entrepreneurs in Geneva, the Jura and the Valais.

The FDPIC also answered specific enquiries about the new Federal Act on Data Protection directly by email and via his telephone hotline. Interest was high, with the number of telephone enquiries in August and September reaching double the figure of previous months.

New FDPIC website

During the year under review, the FDPIC completely redesigned his website in view of the entry into force of the new Act in order to meet the demand for written information.

He updated all relevant texts to align them with the new Act, explained the new features of the Act in a number of articles and drew up a one-page summary of the key new features. This includes information on the right to information, the duty to provide information, penal provisions, fee-charging and data protection certification. The FDPIC has also published a list of Frequently Asked Questions on his website, which is constantly being updated.

Guides and fact sheets

The FDPIC also provides practical tools relating to the FADP on his website.

Online portals for secure electronic reporting to the FDPIC

Prior to the introduction of the new Federal Act on Data Protection, the FDPIC introduced reporting portals on his newly designed website that offer data controllers a secure way to fulfil their reporting obligations electronically.

Register of processing activities (DataReg)

Federal bodies register their records of processing activities with the FDPIC via the DataReg register. The new portal replaces the previous solution and no longer includes notifications by private individuals, as was required under the previous FADP. In addition to the migrated entries of the federal bodies, there are a large number of new entries by data controllers and from registers. New entries include, in particular, entries by pension funds and collective foundations, which are classified as federal bodies and make up a large portion of the three thousand entries in the reporting portal to date. The register is publicly accessible.

(Link: www.datareg.edoeb.admin.ch)

Data breach reporting portal

In the event of a data breach that poses a high risk to the data subjects, data controllers can use this portal to report the incident to the FDPIC. The reporting form includes all the information required to submit a report.

Since the online portal was launched, the FDPIC has received a large majority of data breach reports electronically. He has noticed that the portal is being used by operators in a wide range of sectors, from hotels to collective foundations. The FDPIC was particularly interested in cases involving data processors (e. g. hosting companies) as a large number of reports was expected in that area, whereby the FDPIC is keen to adopt a coordinated approach.

(Link: www.databreach.edoeb.admin.ch)

Contact details of data protection officers (DPO portal)

Private individuals who choose to appoint a data protection officer and notify the FDPIC that they have done so will be subject to fewer data protection impact assessment requirements.

Federal bodies are obliged to appoint a DPO. Under Article 27 paragraph 2 Data Protection Ordinance, federal bodies are required to publish their DPOs' contact details online and communicate them to the FDPIC. They may submit the contact details of their DPOs to the FDPIC electronically via this dedicated online notification portal.

To date, almost two thousand data controllers have registered one or more DPOs via the portal.
(Link: www.dpo-reg.edoeb.admin.ch)

DataBreach-Portal

A total of 245 notifications have been received since the online form was introduced on 9 May 2023.

In 57 cases, further information was provided with follow-up notifications, either spontaneously by the data controller or at the FDPIC's request.

In a number of cases, the data breaches reported involved a contract service provider (Xplain, Concevis, Booking.com etc.). These breaches invariably involved a very large number of data subjects being exposed to high risks.

New Ordinance on Data Protection Certification

The new Ordinance on Data Protection Certification (DPCO) came into force on 1 September 2023 along with the revised Federal Act on Data Protection. In the ordinance, the guidelines on the minimum requirements for a management system have been revised, and guidelines have been drawn up on further criteria under data protection law according to which products, services and processes are to be assessed for certification.

The FDPIC worked with the Federal Office of Justice (FOJ) and the Swiss Accreditation Service (SAS) to align the Ordinance on Data Protection Certification (DPCO) with the new Federal Act on Data Protection (FADP).

Certification can now also be provided for services as well as for organisational structures, procedures (management systems) and products.

Although not expressly provided for, the ordinance also considers the possibility of certifying data processing operations, particularly in connection with the certification of products and services. This brings the Swiss certification system into line with European legislation, meaning that Swiss certification of data processing operations will be recognised by European data protection authorities.

There is now a harmonised validity period of three years for certification certificates subject to a mandatory annual review.

Under the FADP, private data controllers are now exempt from the obligation to carry out a data protection impact assessment if their data processing operations are certified accordingly. This replaces the possibility, under previous legislation, of exemption from the obligation to register data collections. The corresponding provisions of the DPCO have been amended accordingly.

All information on data protection certification can be found on the FDPIC's website.

New data processing policy templates

A processing policy needs to be drawn up for certain data processing operations. The aim of this policy is to provide an overview of data processing operations, which can prove crucial when it comes to rectifying data breaches. The FDPIC has published data processing policy templates on his website.

The new Data Protection Ordinance (DPO) came into force on 1 September 2023 along with the new Federal Act on Data Protection (FADP). The new legislation still requires a processing policy to be drawn up for certain data processing operations. The requirements are set out in Articles 5 (for private individuals) and 6 (for federal bodies) of the DPO.

The FDPIC has prepared templates to help data controllers draw up their own data processing policies. There are two different templates: one for federal bodies and one for private data processors. The templates include the necessary content and a sample table of contents.

The data processing policy includes, for example, information flows, the purpose of which is to show which information is shared by the body operating the system with other bodies, when, how and in what form. A carefully drawn up and regularly revised data processing policy is a crucial document, particularly in the event of a data breach, as it provides an overview of the affected data and systems in the immediate aftermath. It can also help to promptly identify damage mitigation measures.

Logging

Logging is regulated in Article 4 DPO and is one of the technical and organisational measures taken to guarantee data security. Although described as a standard procedure, it continues to raise questions. The FDPIC has drawn up detailed technical recommendations on the subject.

During the year under review, the FDPIC received a number of enquiries regarding logging. The concept already existed in the old law (Art. 10 OFADP) and remains largely unchanged. Logging is used to trace data use. This helps to guarantee data security not only by creating a data processing framework (anyone handling data knows that they are leaving a trace) but also by making it easier to understand what happened in the event of an incident. However, the new Article 4 of the Ordinance is more complete and makes logging mandatory for federal bodies, which have three years to bring themselves up to date (Art. 46 para. 1 DPO). Up until now – as is still the case for private individuals – logging was only mandatory for the processing of sensitive data and profiling and when other preventive measures were not sufficient. However, the regulations continue to raise a number of questions and practical difficulties (for example the definition of ‘automated processing’, compliance with the purpose of logging, logging method, old applications with no logging capabilities and new technologies such as AI), which the FDPIC has been asked to clarify.

The FDPIC has issued detailed technical recommendations on the subject, which are available on his website. They provide an overview of what is to be included in the logs and the requirements for technical fulfilment of Article 4 DPO.

New Guide to Technical and Organisational Data Protection Measures

[With the entry into force of the new Federal Act on Data Protection, the FDPIC has updated the Guide to Technical and Organisational Data Protection Measures \(TOM\) on a legal and technical level.](#)

This guide provides data controllers with an overview of the laws that apply to them and a clear description of the various tools, resources and reference material available to help them deploy the necessary measures. The guide has been completely revised to take account of the major changes in the new Federal Act on Data Protection (FADP), evolving standards and state-of-the-art technology.

In particular, the guide explains the new definitions of terms used in the FADP, including the key concepts of ‘high risk’ and ‘profiling’, and introduces new tools, namely a code of conduct and certification. It presents the key tools of the new law, namely the data protection impact assessment (DPIA) and the role of the data protection officer, as well as the register of processing activities, and outlines the steps that need to be taken in the event of a breach of personal data security. The guide also covers the requirements that apply specifically to data processing by federal bodies.

The main themes of data protection are presented from the point of view of possible technical and organisational measures, such as privacy by design and by default, anonymisation and pseudonymisation, along with measures concerning the workplace infrastructure, including advice on the security of premises and server rooms and on using the cloud for processing personal data. The guide also explains the access management policy, identification and authentication measures and remote access (home office) as well as the life cycle of data, measures regarding data input, data security and destruction of data, encryption and logging where required.

The Guide to Technical and Organisational Data Protection Measures is primarily intended for people in charge of information systems – whether technicians or not – who are directly confronted with the problem of personal data management. The guide is available on the FDPIC’s website in the three Swiss national languages and in English.

Data Protection Impact Assessment

Private individuals and federal bodies are required to carry out a data protection impact assessment (DPIA) when the processing of personal data is deemed to pose a potentially high risk to the privacy or fundamental rights of the data subjects.

The FDPIC's DPIA fact sheet provides guidance for private data processors in particular. It defines 'high risk' and provides guidance on preliminary risk assessment and on the structure and content of a DPIA. It also outlines the procedure after completion and the measures taken by the FDPIC. The FDPIC examines the DPIA submitted to him and provides an opinion to the controller. The FDPIC's opinion is merely a recommendation and does not constitute approval or authorisation of the planned data processing operations. However, the FDPIC may open an investigation in his supervisory capacity and order the controller to take any action required.

The Federal Office of Justice provides tools for carrying out DPIAs within the Federal Administration, including a Federal Council directive on a preliminary risk assessment and a data protection impact assessment for data processing operations carried out by the Federal Administration as well as DPIA guidelines.

Investigation procedure

The revised Federal Act on Data Protection strengthens the FDPIC's supervisory powers and declares the Federal Act on Administrative Procedure applicable to investigations that the FDPIC opens ex officio following a report or violations of data protection regulations. Under the new law, the FDPIC is also authorised to order administrative measures to enforce the provisions.

In certain circumstances, the FDPIC is not only authorised but also obliged to investigate. He has published a detailed review of the relevant provisions of the Act on his website and has summarised them in a fact sheet.

The FDPIC provides a notification form for those affected by a data breach. Persons not directly affected may also file a report with the FDPIC.

For data controllers there is a separate contact form, which they can use to request advice or the FDPIC's opinion on specific issues such as the approval of codes of conduct or cross-border disclosure of personal data.

1.2 Justice, Police, Security

INVESTIGATION AGAINST FEDPOL, FOCBS AND XPLAIN

RIPOL access and data breach

The investigations into access to the RIPOL police search system and the data security breach at Xplain AG are well advanced.

On 13 April 2023, the FDPIC launched a preliminary investigation following questions raised by the Aargauer Zeitung on 11 April 2023 concerning the legality of access by employees of the Federal Office for Customs and Border Security (FOCBS) to the national police search system RIPOL operated by the Federal Office of Police (fedpol). During the preliminary investigation, the two federal offices submitted written statements on the facts of the case. Based on this feedback, the FDPIC opened a formal investigation into both federal offices regarding RIPOL access. The two federal offices answered a list of questions from the FDPIC and showed him the data processing operations in question in accordance with Article 27 para. 3 old FADP. These two procedures were

subsequently suspended until conclusion of the procedure described below concerning the data breach incident at Xplain AG.

At the beginning of June 2023, the two federal offices fedpol and FOCBS informed the FDPIC that their collaboration with Xplain AG had led to data breaches that posed potentially high risks to the data subjects concerned. On 20 June 2023, the FDPIC opened further formal investigations into the two federal offices relating to this data breach (see press release of 21 June 2023). The procedures were extended to Xplain on 13 July 2023 (see press release of 14.07.2023). During the investigations, the FOCBS and fedpol answered a list of questions regarding the data breach.



Documents were issued by the parties to the procedure. In addition, hearings were held with the parties involved and the National Cyber Security Centre (NCSC) so that the FDPIC could gain a clearer understanding of the facts of the case. The FDPIC is prioritising the data breach investigation at Xplain AG, which he expects to conclude shortly.

CYBERATTACK

Preliminary investigations regarding Concevis

The FDPIC launched two preliminary investigations following a cyberattack on the company Concevis: one at the company itself and one at the Federal Statistical Office. The investigations are still ongoing.

Concevis fell victim to a ransomware attack in November 2023. The company provides software solutions to public administrations. The data affected by the attack includes data from the Swiss Federal Statistical Office (FSO). As a result, the FDPIC launched two preliminary investigations – one at Concevis and one at the FSO – in mid-November. The aim of these preliminary investigations is to carry out an initial assessment from the perspective of the FADP in order to establish whether there may have been any failures and, if so, the extent of such failures.



The FDPIC calls for compliance with data protection rules in the digitalisation of police administrative assistance

In winter 2023-24, the Conference of Cantonal Justice and Police Directors (CCJPD) held a consultation on an agreement on the sharing of police data, in which the federal government was to be involved, which the FDPIC criticised both during the consultation and in the media. The FDPIC insisted that the principle of proportionality and citizens' claims for legal protection be observed. The proposed agreement aims to establish a common police data space accessible via a search platform. The platform would enable cantonal police forces to submit online requests for access to information on persons recorded by cantonal police but not yet entered in national police systems without having to meet specific criteria. At present, information requests are considered on a case-by-case basis in a partially automated administrative assistance process.

Under the agreement as it was worded at the time of going to press, information regarding administrative police authorisations and measures, and minor incidents such as distur-

bances of the peace would be directly accessible on an inter-cantonal basis. As the federal government would effectively be a party to the agreement, the same information would thus also be directly accessible to the federal police authorities. To date, these have dealt predominantly with complex and serious criminal offences and security threats.

The scope of application of the proposed agreement covers the entire spectrum of preventive and repressive police action, and the agreement does not provide for sufficiently specific purposes for the processing and sharing of personal data between police forces: therefore, the new platform is expected to bring about a systemic change in police data flows and processing powers at all levels of the federal state (communal, cantonal and federal levels). The same applies to data protection, as the agreement stipulates that data processing on the search platform must be carried

out in accordance with the Federal Act on Data Protection and, if the federal authorities are involved as planned, under the supervision of the FDPIC.

As the overall architecture of the scheme is geared towards the involvement of the federal authorities and has all the hallmarks of a centralised police database, there is significant potential for serious encroachments on the privacy and informational self-determination of citizens. Today's partially automated administrative assistance process via the national police register is subject to a general documentation obligation that enables data subjects affected by the transfer of data to protect their rights. However, online access to all police data without the need to meet specific criteria threatens to substantially further erode this legal protection.

At the time of going to press, it is not known whether the wording of the proposed agreement will include the reservations and qualifications required under data protection law. The same applies to the envisaged involvement of the federal authorities, which, without the necessary reservations and qualifications, also raises federal and constitutional law concerns.

Digitalisation is not a licence to create monolithic superpowers

Administrative assistance

In interpreting the Federal Constitution, doctrine and case law provide for a general duty of the federal and cantonal authorities to support other authorities in the execution of their statutory duties by providing administrative assistance. The main form of administrative assistance provided today is the reciprocal sharing of information regarding specific cases. Where personal data is involved, the sharing of such data is governed by the provisions of federal and cantonal data protection legislation, subject to special statutory provisions.

Online access to personal data

It is current common practice for federal and cantonal legislators to instruct the authorities of their communities to grant other authorities of the same or other communities online access to certain parts – but never to all – of the data they process.

According to the current practice of the FDPIC, where other authorities are granted online access to personal data, compliance with data protection rules is assessed based on the following criteria:

- Firstly, in **qualitative** terms, the legal bases need to specify that the other authority must only be granted access to certain categories of data in accordance with the principle of proportionality: these categories need to be limited in order to ensure the processing of data for sufficiently specific purposes;

- Secondly, it must be proven in **quantitative** terms, based on a quantity structure, that the online access granted is appropriate and necessary. This is the case if, without online access, each of the tasks of the other authority for which assistance is required leads to an accumulation of manual or partially automated requests for administrative assistance with similar or identical justifications. In addition, the group of persons authorised to access the data must be limited to those members of the other authority's staff who have the necessary training and specialisation to carry out the tasks requiring assistance in accordance with the law;
- Thirdly, a data protection impact assessment is required for large projects as these have the potential to seriously encroach on the fundamental rights, privacy and the right of access to the courts of a large number of people due to the extensive scope and high rate of online data sharing and the sensitive nature of the data shared.

Online networking of authorities

During the various consultation procedures that took place during the year under review, the FDPIC was again confronted with a large number of bills that provided for the online sharing of sensitive personal data under the responsibility of or with the significant involvement of the federal authorities.

It became clear that project managers are finding it increasingly difficult to justify the online networking of authorities based on the requirements set out above. Instead, they argue that the online networking of authorities is consistent with the current need for digitalisation of administrations according to what is technically feasible today and as such requires neither special justification nor restrictions in terms of scope or purpose.

Monolithic superpowers

The FDPIC must oppose arguments that amount to a dictate of what is technically feasible as they conflict with the principle of legal certainty and the data protection principles of legality and proportionality. He urgently warns against authorities with fully or partially overlapping tasks sharing all of the data they collect on citizens and thus freely networking across all jurisdictional boundaries of the constitutional state, which is organised in a power-sharing manner in geographical and substantive terms. Such a scenario would ultimately lead to a situation in which the specialist authorities that currently serve citizens by providing a public service would eventually merge into 'monolithic superpowers' that are all-knowing in their dealings with citizens.



1.3 Economy and society

ONLINE CAMPAIGN TO GAUGE PRIESTS' CORE BELIEFS

Investigation into the 'Bürgerforum Schweiz'

'Bürgerforum Schweiz' operates an online campaign ('Pfarrer-Check') to gauge priests' core beliefs. It uses a questionnaire to find out which priests and other people working in the church environment share the core beliefs of the 'Bürgerforum'. Recipients of the questionnaire and their responses are published in an online database along with other information. The FDPIC launched an investigation in the last quarter of 2023. During the year under review, the FDPIC became aware of the data processing activities of the 'Bürgerforum Schweiz' relating to its online belief-gauging campaign following an enquiry by the 'Bürgerforum' itself as well as reports from citizens. It collects personal data from 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 core beliefs of the 'Bürgerforum'. The fact that it had set up a publicly accessible database containing the information collected raised concerns. Following the refusal of the 'Bürgerforum' to comply with requests for deletion submitted by data subjects whose data had been published on the campaign website, the FDPIC initially intervened informally, demanding that the deletion requests be complied with and that the information provided in the questionnaires only be published with the data subjects' express consent.

The 'Bürgerforum' accepted our request to only publish the responses of individuals who had expressly consented to this in advance. However, it argued that its processing of personal data could be justified by an overriding public interest. Therefore, even if a data subject objected to their data being processed because they did not wish to be present in the database, their data would not be deleted.

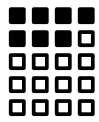
In December 2023, the FDPIC launched a formal investigation into the data processing activities in question in order to assess compliance with data protection law. Under the new legislation, he first established the legally binding facts as part of an administrative procedure and then concluded the procedure with a decision.

TENANCY APPLICATION FORM

Preliminary investigation at a property management company

As part of an informal preliminary investigation, the FDPIC drew the attention of a property management company to criteria in its tenancy application form that were questionable from a privacy perspective, whereupon the company promptly revised its form. As well as asking for the personal details and financial standing of prospective tenants – a reasonable and legitimate request – the tenancy application form requested proof of pregnancy. The landlord argued that this request had to be assessed in the context of the housing shortage in cities. It allowed the landlord to also allocate larger flats to applicants who were in the process of planning a family but did not yet have any children, so that they would not be at a disadvantage compared to families with children. Besides, the data was deleted when applications were rejected.

The FDPIC makes it clear that the data processing operations of property management companies need to comply with the principles set out in Article 6



FADP, in other words they must be proportionate and carried out for a specific purpose.

Property management companies are entitled to collect and process personal data provided that they do so within the bounds of what is objectively reasonable and necessary for selecting suitable

tenants and that their actions do not constitute an excessive invasion of privacy. The processing of personal data relating to the pregnancy of a prospective tenant clearly falls outside these bounds. It is also not clear how such data processing could be justified by an overriding interest of the property management company or by the

data subject giving their consent, as consent must always be voluntary and informed, which is hard to imagine would be the case in the tenancy application process given the housing shortage.

The property management company was urged to ensure that its data processing operations complied with the law, to modify its application form accordingly and to immediately delete any data that it had already collected.

The property management company complied with these requests within the set deadline.

Investigations of the FDPIC

The FDPIC will open a formal investigation ex officio or following a report if there are sufficient elements to suggest that data processing activities may violate data protection regulations unless the violation is minor.

Before launching an investigation, the FDPIC has the option of taking informal action as a first step.

In principle, the FDPIC pursues a resource-efficient solution-oriented approach in his investigations. The aim is to ensure that any breach of privacy is swiftly remedied. Today, data subjects are aware of their privacy rights, and companies are aware that compliance with data protection regulations is a key element in their relationship with customers.

When the FDPIC becomes aware of a potential breach of privacy, his first step is often to informally alert the data controller to the possible misconduct. In the FDPIC's experience, data processors are very often prepared to take swift action to remedy the situation.

In their response to the FDPIC, the data controllers contacted are free to comment on the allegations and express their views on the facts of the case and the legal situation. In informal preliminary investigations, data controllers are under

no legal obligation to act on the FDPIC's comments.

If an informal exchange fails to yield a satisfactory and legally compliant solution, the FDPIC is entitled to launch a formal investigation at any time, during which he will examine in detail the facts of the case and the legality of the personal data processing operations in accordance with the Federal Act on Administrative Procedure. After hearing the data controllers, who are obliged to cooperate, he will then take any administrative measures required.

Final report including recommendations

During the year under review, we completed our case investigation into the auction platform Ricardo, which we had started in 2017, and issued recommendations. We concluded that, in the specific circumstances, the data processing carried out by Ricardo and the TX Group – in particular the transfer of data and cross-platform tracking for the purpose of targeted advertising – needed to be justified by the data subject's explicit consent. The privacy policy also needed to be improved.

The FDPIC had already presented some of his findings regarding the facts of the case in his 28th Annual Report (see 28th Annual Report, Section 1.4).

After a consent management platform was introduced on the Ricardo website and the Swiss Marketplace Group (SMG) was established, the FDPIC examined the impact of these technical and organisational changes on the data processing operations analysed as part of the investigation (see 29th Annual Report, Section 1.3).

Ricardo and the TX Group had announced that the data processing, data flows and data controllers would

remain the same after reorganisation and that the new operators – the SMG companies and their shareholders – would not take part in the data transfer, and therefore it was decided in 2022 that the case investigation did not need to be modified or extended. However, during the year under review, it emerged that, in addition to data being transferred between Ricardo AG and TX Group AG – which was the subject of our investigation – data was also being transferred within SMG. According to the FDPIC, it would not be practical to formally extend the already advanced procedure to SMG in order to investigate the transfer of data within SMG. Should this prove necessary, the FDPIC will launch a new investigation under the revised law.

To ensure that his conclusions reflected, as far as possible, the current state of affairs, the FDPIC included the publication of a new privacy policy and the introduction of a consent management platform on the Ricardo

website in his findings. Ricardo and the TX Group were asked to verify the accuracy of this addition. Based on this, the FDPIC carried out a legal assessment of the facts.

From a substantive point of view, the FDPIC concluded that the data processing carried out by Ricardo and the TX Group for the purpose of targeted advertising constituted a violation of privacy that could not be justified by any overriding interests of the two data processors. The transfer of data by Ricardo and the cross-platform track-



ing by the TX Group would need to be justified on a case-by-case basis by the data subject's explicit consent, which needed to

be given voluntarily after the person had been adequately informed. As data processing can lead to the creation of personality profiles, the FDPIC recommended that users be informed individually in advance about the transfer of data to the TX Group and cross-platform data linkage for the purpose of targeted advertising, and users would need to give their express consent. The information in the privacy policy also needed to be improved.

The FDPIC submitted his final report to Ricardo and the TX Group for review and comment.

CUSTOMER DATA

Investigation into Digitec Galaxus

In spring 2021, the FDPIC opened a procedure to inspect the processing of customer data at Digitec Galaxus, one of Switzerland's largest online stores. In his final report, he states that the principles of transparency and proportionality have been violated and issues a number of recommendations.

Following an informal preliminary investigation, the FDPIC opened a procedure against Digitec Galaxus in spring 2021 to inspect its processing of customer data in order to verify compliance with data protection regulations (see 28th Annual Report, Section 1.4, and 29th Annual Report, Section 1.3). The investigation was prompted by reports from data subjects stating that they were required to accept all data processing activities described in the online store's privacy policy before they could go ahead and place an order. The operator rejected subsequent objections raised by data subjects with regard to their personal data being processed as described in the privacy policy on the grounds that the privacy policy applied to everyone equally without exception.

In a thorough clarification of the facts of the case, the data controller stated that a number of processing operations mentioned in the privacy policy were not actually carried out at all. Furthermore, data subjects' right to

object was fully respected in that they could opt not to place an order or request deletion of their personal data. The



data processing operations carried out via the website – in particular the obligation to set up a customer account and the analysis

of customer and purchasing behaviour – were said to comply with the data protection regulations and therefore did not require any justification.

The FDPIC checked whether the information in the privacy policy met the legal requirements in terms of transparency. He also examined the extent to which certain data processing operations could be considered proportionate if they were carried out against the express wishes of data subjects.

In accordance with the transitional provision set out in Article 70 FADP, the facts of the case were assessed under the previous law. Therefore, the FDPIC based his recommendations on Article 29 para. 3 of the FADP of 1992 (see 30th Annual Report, box on p. 20).

After a thorough review, in his final report the FDPIC concluded, among other things, that the operator was violating the principles of transparency and proportionality, as a result of which he issued a number of recommendations to remedy the data processing deficiencies.

In its statement, Digitec Galaxus noted that some of the recommendations to increase transparency had already been anticipated by the introduction of a new privacy policy during the ongoing proceedings. It rejected some of the recommendations. In one of the recommendations, the Commissioner suggested an adjustment to data processing that does not interfere more than necessary with the informational self-determination of its customers. In the opinion of the Commissioner, one possibility would be to offer an alternative guest purchase, i.e. a purchase that can be made on the online platform without registration. Digitec Galaxus accepted this recommendation and will submit corresponding implementation proposals to the FDPIC.

As soon as these are available, the FDPIC will examine whether and to what extent he will take action against processing operations that are the subject of rejected recommendations or recommendations that have not been implemented in accordance with the law.

DATING APP

Case investigation concluded at Once Dating AG

The FDPIC has concluded his procedure against the Swiss-based but internationally operating provider of the Once dating platform. After the company sold the platform, it confirmed to the FDPIC that it had either transferred or deleted the data of its former customers in accordance with data protection regulations.

In spring 2021, the FDPIC launched an investigation into the data processing activities of the Once dating app. In particular, he was keen to determine whether the handling of deletion requests and the disclosure of personal data to third parties complied with

the data protection regulations (see 28th and 29th Annual Reports, Section 1.1 respectively, and 30th Annual Report, Section 1.3).

In his final report of 17 May 2023, the FDPIC issued a number of recommendations aimed at remedying the shortcomings identified and ensuring compliance with the data processing principles set out in the Federal Act on Data Protection. Once Dating AG took the recommendations on board and informed the FDPIC that the platform had since been sold to a foreign company (see press release of 13 June 2023). It also informed the FDPIC that it had promptly deleted all inactive customer data before the takeover. Active customers of the Once dating app had been informed of the takeover and had been given the option to migrate to the platform operated by the legal successor. The new owner was said to have taken note of the FDPIC's recommendations regarding the platform. The FDPIC has therefore concluded his investigation.

TRACKING TECHNOLOGIES

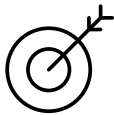
Concerns over Oracle America allayed: Swiss residents unaffected by controversial data processing

The data processing operations over which Oracle America, Inc. is facing a civil lawsuit in the US do not affect people in Switzerland. The FDPIC has concluded his investigations and has decided not to launch a formal investigation.

The FDPIC informed the public on 27 September 2022 that he had taken note of the allegations made against Oracle America, Inc. (hereafter: Oracle America) in a US class-action lawsuit and had examined them for possible invasions of privacy affecting Swiss

residents. According to the lawsuit, Oracle America has been using tracking technologies to collect data on 5 billion internet users and storing it in a database. It is claimed that the data collected is analysed and used by Oracle America to create a database of the data subjects (see also 30th Annual Report, Section 1.3).

The FDPIC investigated the allegations brought against the company and contacted both Oracle Schweiz GmbH and Oracle America to ask questions. In particular, he wanted to know how Oracle America had implemented paragraph 7 of the Oracle Advertising Privacy Policy in order to ensure that no



information on individuals in Switzerland was used for advertising purposes.

Oracle America assured the FDPIC that it no longer offered its services as a data broker for data providers in Switzerland and that it had already terminated all contracts with data providers that supply data specifically on individuals in Switzerland years ago. Furthermore, Oracle America provided credible assurances that it had taken technical measures to prevent data relating to individuals in Switzerland

from being used for advertising purposes and confirmed that Oracle's advertising services did not involve the processing of any information relating to individuals in Switzerland other than the anonymisation and subsequent deletion of data to prevent it from being used for advertising purposes. The company also confirmed that it did not process any information on Swiss residents in connection with the Oracle ID Graph service, nor did it process any offline information on them. In addition, the FDPIC noted that Oracle America had discontinued all 'AddThis' services on 31 May 2023.

As a result, the FDPIC concluded his investigations and, in a statement issued on 6 October 2023, declared that he would not be bringing formal proceedings.

Introduction of a register of beneficial owners

[The introduction of a federal register of beneficial owners of legal entities and other targeted measures is intended to strengthen the system for combating money laundering, terrorist financing and financial crime and is being implemented in accordance with current international standards. The FDPIC oversaw the legislative project, and some of his comments were taken on board.](#)

On 12 October 2022, the Federal Council instructed the Federal Department of Finance (FDF) to work with the Federal Department of Justice and Police (FDJP) to prepare a bill on the transparency of legal entities (LETA) by summer 2023, intended to facilitate the identification of the beneficial owners of legal entities and thus strengthen and modernise important components of the system for combating financial crime. The consultation on the LETA took place from 30 August to 30 November 2023.

The FDPIC shared his views during the office consultation. As a result, the project was improved from a data protection perspective, for example more details were provided as to the content of the new federal register of beneficial owners.

However, the FDPIC's concerns regarding various points of the LETA were only partly addressed when the bill was finalised. The purposes of the Act were only specified with examples

ECONOMY

(with the wording ‘in particular’), whereby the FDPIC criticised the lack of certainty regarding the scope of application. The FDPIC also pointed out on several occasions that any access to the register by an authority needed to have a clear purpose and be proportionate. Therefore, any online access by an authority, such as the Federal Statistical Office or the Intelligence Service, required clear justification. We also found the provision on profiling to be insufficiently specific.

Furthermore, in the office consultation, the FDPIC demanded in vain that the FDF at least carry out a preliminary assessment as to whether or not a data protection impact assessment was needed before introducing the register and providing online access to various authorities, and that it present its findings in the explanatory report. The offices in charge chose not to do so: Without a data protection impact assessment, certain data is missing that is needed for proper regulation.

In the second office consultation (March 2024), the FDPIC found that the associated risks are potentially high and that online access is not sufficiently justified in either quantitative or qualitative terms. (see also Section 2.4)

New legislation to screen foreign investments

On 15 December 2023, the Federal Council adopted the dispatch for a federal act on the screening of foreign investments. During the office consultation, the FDPIC focused on compliance with data protection requirements.

Investment screening is intended to prevent takeovers of Swiss companies by foreign investors in cases where the takeover could threaten or jeopardise Switzerland’s public order or security.

To this end, the draft Investment Screening Act provides that takeovers of Swiss companies shall require SECO approval. This applies to companies that operate in particularly critical sectors and that are intended to be taken over by state-controlled foreign investors.

Greater transparency

During the office consultation on the dispatch on the Investment Screening Act, the FDPIC focused on compliance with data protection requirements, as he had already done during the office consultation on the preliminary draft. For example, with regard to cooperation between SECO and national authorities, the FDPIC succeeded in obtaining a clearer statement as to what data is disclosed to whom, by whom, how and for what purpose.

Extended right of appeal

The FDPIC also criticised the regulation of legal protection, which had previously restricted the right of appeal to the foreign state investor and the Swiss company. The new draft legislation stipulates that this restriction on the right of appeal does not apply in the presence of a SECO-issued information or disclosure order. As a result, legal action can now be taken not only by the foreign state investor and the Swiss company but also by other stakeholders in the takeover who may wish to appeal a SECO-issued information order.

1.4 Health

SUPERVISION OF THE HEALTH INSURANCE INDUSTRY

Exchanges between the FDPIC and the FOPH

The FDPIC and the FOPH have established regular exchanges as part of the implementation of the recommendations issued by the Swiss Federal Audit Office on coordination in the supervision of health insurance companies.

During an audit carried out at the Federal Office of Public Health (FOPH) on supervision of the insurance industry, the Swiss Federal Audit Office (SFAO) found that the FDPIC and the FOPH needed to clarify their roles and establish communication and coordination between the two offices (Audit CDF-20424). Health insurance companies must comply with the provisions of social security law and data protection law when carrying out their activities. Consequently, they are subject to supervision by both the FOPH and the FDPIC.

The FDPIC welcomed coordination of the supervisory activities of the FOPH and the FDPIC in relation to health insurance – given their overlapping responsibilities – as well as the clarification of their roles and responsibilities. However, he pointed out that the FDPIC’s independence had to remain unaffected by the efforts to coordinate supervision and that he would continue to carry out his supervisory duties vis-à-vis the FOPH. As a first step in implementing the SFAO’s recommendations, the FDPIC and the FOPH worked together to revise the FOPH Circular no. 7.1 on the supervision of health insurance companies (see 29th Annual Report, Section 1.6).

In a second step, the FOPH and the FDPIC established regular communication in order to ensure that the supervision of health insurance companies was able to benefit – as envisaged by the SFAO – from the experience and proximity of the FOPH (through on-site inspections) and from the FDPIC’s enhanced legal powers under the revised FADP. As result, the two offices were able to coordinate the following activities:

- Responses to the entry into force of the revised Circular no. 7.1 on supervision;
- Introduction of the obligation for service providers to send a copy of their invoices to the insured persons;
- Requests from insurance companies for access to the employment contracts of persons employed in home help and care services;
- GP access to insurance medical advisors;
- Data protection aspects in the development of care centres bringing together different healthcare providers; and
- Insurance certificates for the tax authorities: here, it was pointed out that the tax authorities did not need to be given details of the health services provided but only the amounts of the premiums and medical expenses.

The FDPIC and the FOPH also exchanged views on their current inspection activities in the insurance sector.

- The creation of new insurance apps and platforms;
- The development of new insurance models;
- The outsourcing of health data;

VACCINATION DATA

Project to recover data from the meineimpfungen.ch platform

The FDPIC provided administrative assistance to the Canton of Aargau's freedom of information and data protection officer after the data of the former meineimpfungen.ch platform was taken over by the parent organisation eHealth Aargau. Partly funded by the FOPH, the project aimed at returning at least some of the vaccination data is now scheduled to begin in spring 2024 at the earliest.

Operated by a private foundation and heavily subsidised by the federal government, the meineimpfungen.ch platform was found to have serious data protection deficiencies, which prompted the FDPIC to conduct formal proceedings in March 2021, which he concluded in August of the same year by issuing formal recommendations. The foundation was unable to rectify the deficiencies and the lack of data integrity, as a result of which bankruptcy proceedings were started against the foundation in November 2022. Given the high risk that the data that had become part of the bankruptcy estate would be auctioned off, the FDPIC worked with the data protection officer of the canton

of Bern to demand that the bankruptcy office of the Bern/Mittelland district delete the data. After the Department of Health and Social Affairs (DGS) of the Canton of Aargau and the Federal Office of Public Health issued a written agreement that they would comply with data protection regulations, the FDPIC reiterated his recommendation that the data be deleted. The data was then transferred to the Canton of Aargau to determine whether it could be returned to the data subjects. (The FDPIC reported in detail on this matter in his last two annual reports: 29th and 30th Annual Reports, Section 1.4 respectively).

As part of a preliminary project, the parent organisation eHealth Aargau (SteHAG) – which had been instructed by the Canton of Aargau to recover the data – initially concluded that it would be possible to return the vaccination data to the former platform users. In May 2023, the project managers

announced that a project had subsequently been set up to create the technical framework for the data to be returned in compliance with data protection regulations.

On 11 December 2023, SteHAG announced that the project – partly financed by the FOPH – could not begin until spring 2024 at the earliest, leading to a further delay in the return of the vaccination data – now almost three and a half years old – to the data subjects.

Since the data was transferred to the canton of Aargau, the canton's freedom of information and data protection officer has been responsible for supervising data processing. The FDPIC has forwarded the findings of his procedures relating to the vaccination platform to his cantonal counterpart by way of administrative assistance.

In light of the findings of the meineimpfungen.ch case, the FDPIC also commented on other occasions that when private companies are commissioned or subsidised to provide digital services to the Swiss Confederation, federal security standards must be agreed, implemented and monitored.





MEDICAL PRACTICE

Patients required to sign a new consent form

During the year under review, the FDPIC received a number of enquiries regarding the consent form that healthcare professionals have been asking patients to sign since the new FADP came into force. This new practice, and specifically the need to sign such a document, has raised many questions among patients. A number of medical organisations and umbrella organisations are providing their members and partners with a sample consent form. The purpose of the form is generally twofold: Firstly, to inform patients in a clear and transparent manner about how their data will be processed in accordance with the requirements of the Federal Act on Data Protection, with particular regard to the purposes for which it will be processed and any planned disclosure of their data to third parties (e.g. to

another physician, a billing company etc.), so that patients are aware and are in a position to give valid consent. Secondly, the consent form allows professionals to obtain the patient's express consent where required, for example for the disclosure of sensitive data, which includes data relating to the indi-



vidual's health. According to the law, neither information nor consent need to be in writing, but a person's wishes need to be

sufficiently clear. However, in practice, the written form is often preferred for evidence or documentation. By signing the document, patients certify that they have been informed and that they consent to their data being processed to the extent described. In accordance with the principle of proportionality, however, only the personal data that third parties need in order to achieve the legitimate processing purposes will be disclosed, preventing bulk disclosure of data.

At the same time, health data is also subject to medical secrecy, meaning that any communication of patient data to third parties requires the patient's prior consent, subject to criminal prosecution (Art. 321 Swiss Criminal Code) and legal obligations to communicate data to the authorities or third parties.

Patients are free to decide whether or not to sign the form. However, it is important to bear in mind that professionals need patients' consent in order to pass on their health data to third parties and also have an understandable interest in having a written document certifying that the patient has been duly informed. Furthermore, refusal to sign or deletion of certain clauses can lead professionals to refuse treatment because of the legal uncertainty in which they may find themselves.

Therefore, if any parts of the form are unclear or seem excessive, or if any questions remain, the FDPIC recommends contacting the person who issued the form for clarification.

DATA REUSE

The Federal Act on Data Protection versus the Federal Act on Research Involving Human Beings

The Federal Act on Data Protection (FADP) and the Federal Act on Research Involving Human Beings (HRA) both deal with the reuse of data for research purposes. Consequently, the overlap between the two acts is a recurring issue.

Over the past year, the FDPIC has often had to address the issue of the overlap between the FADP and the HRA, be it in office consultations or in advising individuals or federal bodies.

The FADP and the HRA sometimes deal with similar issues, for example the case of data collected previously for other purposes being reused for research (for example when a doctor wishes to send a patient's test results to researchers). These situations are regulated by Article 31 para. 2 let. e and Article 39 FADP (applicable to private individuals respectively federal bodies) and Article 32 ff. HRA.

The HRA is a special act compared with the FADP and therefore takes precedence over the FADP in matters that fall within its scope, essentially research on human diseases or on the human body, on persons (including

deceased persons, embryos and foetuses), on biological material or on health-related personal data. It should be noted that the HRA only regulates certain aspects of data processing, and the FADP still applies to all other aspects that are not specifically regulated in the HRA.

Specifically, one of the key differences between the two regimes is the basis on which reuse is justified, namely an overriding interest on the part of the controller (Art. 31 para. 2 FADP) or the law itself (Art. 39 FADP) in the FADP versus consent (to varying degrees) in the HRA.

Generally speaking, the HRA regime may appear more complex than that of the FADP. However, this is justified by the subject matter, namely research involving human beings, by definition a sensitive area. In this context, the standard mechanism of Article 31 para. 2 FADP would be inappropriate as it would involve the controller (means the doctor, acting as both judge and party) weighing up the interests themselves. The more specific framework of the HRA therefore allows greater account to be taken of the individual's wishes, better information to be provided and, generally, greater legal certainty in the interests of data subjects and researchers.

Comprehensive revision of the Federal Act on the Electronic Patient Record

[The Federal Council intends to drive forward the development of electronic patient records and introduce specific measures to promote their dissemination and use. To this end, it submitted for consultation a proposal for a comprehensive revision of the Act in June 2023, which includes a number of major changes. The FDPIC commented on some key points.](#)

The draft revision marks a paradigm shift: Whereas the current Act on the Electronic Patient Record (EPRA) provides for free consent to the opening of an electronic patient record (EPR), the draft revision proposes a move from a system of explicit consent (opt-in)

to one of presumed consent with a right to object (opt-out), meaning that from now on, anyone domiciled in Switzerland with compulsory health-care insurance will need to have an electronic patient record unless they have expressly refused one after being informed. Any refusals will be recorded in a register. If no objection is raised, an EPR will be opened and may be completed or managed by healthcare professionals and by the patient themselves, who will be able to decide who may access it. The revised Act also effectively obliges all healthcare providers to join a certified community or reference community and to record data relevant to the treatment of patients in the EPR in order to make it available to other healthcare professionals.

As the data protection supervisory authority, the FDPIC is of the opinion that the current model – namely prior consent to the opening of an electronic patient record – better guarantees the right to self-determination of data



subjects, i.e. the right of every individual to be able to determine for themselves whether or not they wish to have an electronic

patient record and the purpose for which information about them (e.g. health-related information) may be processed. If the opt-out model were to be introduced, however, it

would need to be implemented uniformly in all cantons without excessive bureaucracy.

The revision also introduces other new features that modify or extend the processing of personal data envisaged for the current EPR and increase the risks to the privacy and informational self-determination of data subjects. The FDPIC has therefore invited the Federal Office of Public Health to assess these additional risks and, if necessary, to carry out a data protection impact assessment and present its findings on the matter. If the data is generally only accessible to authorised persons, the patient must be informed of the significance of each authorisation and the hierarchy involved, as well as the option to restrict access. In addition, in accordance with the principle of data

protection by default, it must generally be ensured that the parameters are set to the highest level of confidentiality and that healthcare professionals are not able to access the information without the data subject's express consent. When joining or leaving a group of healthcare professionals, the patient should be systematically informed unless they do not wish to be.

The FDPIC welcomes the fact that health insurance companies are only granted access to record certain administrative data in the EPR with the patient's consent. With regard to the possibility of using EPR data for research purposes, the FDPIC welcomes the fact that the revised Act allows non-anonymised medical data to be made available only with the patient's express consent.

However, he is concerned about the plan to grant third-party health applications access to the EPR. With the patient's consent, health applications will be able to access the EPR and record and / or consult medical data, e.g. via a smartphone or a medical device. The FDPIC believes that the protection and security of patient

data must be guaranteed for all applications. Access to the EPR by certified third-party health applications that have been evaluated as reliable and secure does not pose a risk to patient data or to the operational security of the EPR itself. The use of an interface is only permitted after a thorough risk assessment has been carried out and measures have been taken to mitigate the risks. Furthermore, the transfer of data from the application to the EPR must be sufficiently secure and encrypted.

Given the number of data subjects and the sensitive nature of the data involved, the FDPIC believes that the Act should define in greater detail the remits and responsibilities with regard to data processing.

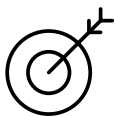
1.5 Employment

EMPLOYMENT LAW

Personnel record-keeping requirements

The obligation to delete personal data that is no longer required and retention of such data in personnel files raises questions for employers. The principle of proportionality is key in answering these questions.

During the year under review, the FDPIC received an increasing number of enquiries regarding privacy compliance in the management of personnel files, particularly with regard to retention periods, storage media and the erasure of personal data. The processing of personal information is permitted in the employment relationship provided that it complies with the general principles of data processing set out in the FADP (in particular the principles of proportionality and limitation of purpose) and the Swiss Code of Obligations. This means that the employer may only process personal data that is required for the fulfilment of the



employment relationship (relating to suitability and performance). It also means that personal data must be deleted if it is not (or no longer) required or once the purpose for which it was processed has been achieved.

Detailed information on retention periods before, during and after the employment relationship and on storage media can be found on the FDPIC's website.

EMPLOYMENT LAW

Data protection rules applicable to pension funds

The FDPIC was asked by numerous pension funds and professional associations to specify which provisions of the FADP applied to pension funds. In the FDPIC's opinion, pension funds act as federal bodies when they provide compulsory occupational pension plans (OPA), while non-compulsory plans are governed by the provisions for private individuals. The question is relevant as federal bodies are required to notify the FDPIC of their processing activities under Article 12 FADP and provide him with the contact details of their data protection officer under Article 10 FADP.

The provision of mandatory occupational pension insurance (compulsory OPA insurance) constitutes a public task falling under the responsibility of the Confederation (a federal task within the meaning of Art. 5 let. i FADP). According to the case law of the Federal Administrative Court, registered pension funds that provide compulsory insurance cover are considered legal entities entrusted with a federal task (BVGer, A-4467-2011, E. 4.2). In order to fulfil their legal obligations in the provision of compulsory OPA insurance cover, pension funds need to process the

personal data of the insured persons. They process personal data in order to fulfil a federal task and therefore act as a federal body when providing compulsory OPA insurance cover.

By contrast, pension fund operations relating to non-compulsory insurance schemes are subject to the specific provisions of the FADP applicable to private individuals provided that the data processing operations are completely separate from their public task and are carried out exclusively within the scope of the non-compulsory scheme. This is the case for pension schemes that exclusively provide non-compulsory insurance cover and are therefore not registered (Art. 48 OPA e contrario). These include, for example, optional personal pension plans 3A and 3B. If it is difficult or impossible to separate the areas, the provisions for federal bodies shall apply to all operations.

Pension funds that act as federal bodies in providing compulsory insurance and as private individuals in providing optional insurance are subject to supervision by the FDPIC. This also applies to comprehensive pension funds, i.e. those that offer both compulsory and optional insurance, depending on whether the data processing operations in question relate to compulsory or optional offerings.

Pension funds as cantonal or communal public bodies

Pension funds for employees of cantons, municipalities, towns and cities that perform tasks relating to occupational

pension schemes and process personal data in this context are generally not considered federal bodies: they are cantonal or municipal public bodies and are governed by cantonal data protection legislation for compulsory OPA schemes and are subject to cantonal or municipal supervision.

Pension fund service companies act as data processors

In practice, pension funds sometimes outsource some or all of their business operations to external companies. The service companies employed act on behalf of the pension fund in the capacity of data processors within the meaning of Art. 9 FADP.

Understanding whether pension funds are considered federal bodies within the meaning of the FADP is also important given that, under Article 12 FADP, federal bodies are required to notify the FDPIC of their processing operations. Accordingly, pension funds accounted for more than 1000 entries in the register of processing activities (Datareg) during the year under review.



1.6 Transport

NUMEROUS PROJECTS

Consultancy and office consultations on mobility

The FDPIC presented his views on transport and mobility on a number of occasions in his project consultancy work and in office consultations. He calls on state-licensed public transport operators to ensure that passengers can continue to travel anonymously and pay in cash and that they are not penalised by forgoing benefits or facing administrative burdens if they choose to do so.

During the year under review, the FDPIC advised private individuals and federal bodies on mobility issues. A key concern was that companies providing passenger transport – when it is legally regulated task of the state – should continue to ensure that passengers can travel anonymously throughout Switzerland. Furthermore, providers of data-based services should continue to accept cash as a form of payment.

Public transport platform NOVA

In connection with the vulnerability reported in February 2022 in the central public transport platform NOVA operated by SBB on behalf of the Swiss public transport industry organisation Alliance SwissPass (ASP) (see 29th Annual Report, Section 1.7), the FDPIC drew SBB's attention, among other things, to the requirement of proportionality in data retention. Deletion deadlines had not been fully met at the beginning of the reporting year. SBB's data protection team carried out an audit at the end of the reporting year to determine whether the deletion rules had been fully observed on the NOVA platform. If

the audit identifies any deficiencies, the FDPIC will work to ensure that these are rectified in full.

Furthermore, the industry has developed binding IT security standards effective from 1 January 2024, which transport companies that use the NOVA platform are required to implement. Transport companies that already use the platform will be granted a one-time transition period and will be required to provide proof of compliance by submitting a self-assessment by the end of June 2024 at the latest. Any shortcomings identified are to be documented by the companies concerned and rectified by the end of 2024.

SBB customer frequency measurement system

With regard to SBB's customer frequency measurement system 2.0 (KFMS 2.0) project, which had sparked speculation due to the inaccurate wording of the call for tenders (see 30th Annual Report, Section 1.6), SBB submitted a data protection impact assessment (DPIA) to the FDPIC, as agreed in consultation with the latter. Based on the DPIA and information provided by SBB, the FDPIC concluded that at no point was any data generated that could potentially

be misused in such a way as to pose a potential risk. Therefore, he deemed the customer frequency measurement system in its current form to be compliant with data protection regulations.

SwissPass pilot project for collecting 'distribution keys'

Alliance SwissPass requires certain data in order to be able to distribute the revenue from flat-rate tickets such as the GA travelcard fairly among the transport operators. This 'distribution key' is now to be collected digitally, and customers will be invited to take part in the online collection of data relating to their use of the GA travelcard. In order to take part, they need to install a third-party tracking app (e.g. of a market research institute) on their mobile phone which records the location of their mobile phone at regular intervals. To calculate their travel routes, the smartphone sends the market research institute the recorded location data among other things. The recorded journeys are then sent in anonymised form to the Alliance SwissPass (ASP) office, which assesses the journeys and can then calculate the GA travelcard distribution key. The market research institute then deletes the personal data.

The FDPIC pointed out to SBB, among other things, that special attention needed to be paid to data security when implementing this project as the collection of digital data posed additional risks. When choosing a market research institute, data protection had to be the foremost consideration (e.g. a server located in Switzerland). The data protection principles of purpose limitation and transparency were also to be observed at all times.

PNR DATA

Automated driving

The FDPIC presented his views on automated driving on several occasions, for example in the FEDRO office consultation on the corresponding ordinance. We worked to ensure that the intended purposes were achieved without the processing of sensitive personal data or high-risk profiling. The FDPIC also pointed out the need to determine in good time whether a data protection impact assessment was needed for legislative projects. FEDRO informed the FDPIC that our suggestions had been largely taken on board in the draft ordinance.

Video surveillance on public transport

A number of licensed bus companies and manufacturers of public transport vehicles contacted the FDPIC to ask how a full interior and exterior video surveillance system for new buses could be designed in compliance with data protection regulations. In addition to the sufficiently specific legal framework, the principle of proportionality needs to be observed, and data subjects need to be made aware that they are being filmed. They must also know whom they may contact for information in order to be able to exercise their rights as data subjects.

Office consultation on the Passenger Name Records Act

[The FDJP has revised its draft legislation on Switzerland's use of passenger name records \(PNR\) and has held a second office consultation, during which the FDPIC expressed his views.](#)

PNR data is personal information provided by passengers to airlines or travel agencies whenever they book a flight. It is used to combat terrorism and serious crimes, for example by running it through the relevant law enforcement databases. Many European countries have already set up Passenger Information Units (PIUs) to collect, store and process airline passenger data.

The FDPIC expressed his views again in this second office consultation during the year under review (first office consultation: see 29th Annual Report, Section 1.7, and 28th Annual Report, Section 1.8). Among other things, he pointed out that for legislative projects from 1 September 2023 onwards (date of entry into force of the revised FADP), data processing operations needed to be examined in good time in order to determine whether they could potentially pose a high risk to the privacy or fundamental rights of data subjects, in which case a data protection impact assessment was needed. The latter must be submitted to the FDPIC for comment prior to the office consultation.

The FDPIC also emphasised that the data processing principles set out in the FADP, such as the principle of proportionality, were to be observed at all times during the legislative project and its implementation. For example, it was important to ensure that, in the event of false positives, individuals who met the risk profile criteria but are not classified as suspicious would not be flagged as suspicious in the system and that data would be immediately pseudonymised and then deleted. The concerns of the FDPIC with regard to the DPIA have been taken on board and are reflected accordingly in the dispatch.



1.7 International

EUROPEAN UNION

EU adequacy decision

On 15 January 2024 the European Commission confirmed that Switzerland offers an adequate level of data protection.

In its report of 15 January 2024, the European Commission recognises that Switzerland's legislation continues to provide an adequate level of protection for the processing of personal data. Personal data from a Member State of the European Union (EU) or the European Economic Area (EEA) may continue to be transferred to Switzerland without the need for additional guarantees to ensure an adequate level of data protection, a matter of great economic significance.

Switzerland has held an EU adequacy decision since 2000. This was issued under the previous directive (Directive 95/46/EC) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive was replaced in 2016 by the regulation (EU)2016/679 (General Data Protection Regulation (GDPR)) (see 30th Annual Report 2022/23, page 11).

This is of great significance for Switzerland's competitiveness and attractiveness as a business location.

DATA PRIVACY FRAMEWORK

Framework for data transfers to the US

In summer 2023, the EU and the US agreed on a framework for data transfers from the EU to the US, on the basis of which the European Commission issued an adequacy decision. Switzerland also held talks with the US.

In September 2020, following the CJEU's Schrems II ruling, the FDPIC noted that the Privacy Shield Framework between Switzerland and the US did not offer an adequate level of protection for data transfers from Switzerland to the US despite special protection rights being granted to data subjects in Switzerland (see 28th Annual Report 2020/21, Focus II). Since then, personal data transfers from Switzerland to the US have required additional safeguards within the meaning of Article 16 paragraph 2 FADP, such as data protection clauses, standard data protection clauses or binding corporate rules on data protection.

In July 2023, the EU and the US agreed on a new framework, namely the EU-US Data Privacy Framework (DPF), on the basis of which the EU Commission issued a new adequacy decision for data transfers to the US. However, the adequate level of data protection established therein only applies to personal data that is transferred to certified US companies participating in the EU-US Data Privacy Framework. According to the EU Commission, the DPF addresses the CJEU's concerns raised in the Schrems II ruling as, among other things, access by US intelligence services to EU personal data has been restricted and a Data Protection Review Court (DPRC) has been introduced, which is accessible to EU residents. In turn, the United Kingdom also issued an adequacy decision for the US, namely the UK-US Data Bridge, as an extension to the EU-US Data Privacy Framework.

Switzerland also held talks with the US on a data protection framework. Since the revised FADP came into force on 1 September 2023, the responsibility for assessing the adequacy of data protection in foreign countries and international organisations rests with the Federal Council and no longer with the

FDPIC. The countries and international organisations deemed by the Federal Council to offer adequate protection are listed in the Annex to the Data Protection Ordinance. As a result, additional safeguards within the meaning of Article 16 paragraph 2 FADP are required for data transfers from Switzerland to the US until a corresponding adequacy decision by the Federal Council comes into force and the list of countries in Annex 1 of the Data Protection Ordinance (DPO) is updated. If a new data protection framework is established between Switzerland and the US, the Federal Council's adequacy decision based on this framework will only apply to data transfers to participating certified US companies (as under the EU-US DPF and the former CH-US Privacy Shield), while transfers to non-certified US companies will continue to require additional safeguards within the meaning of Article 16 paragraph 2 FADP.

Convention 108+ has been ratified

Modules one and two of the model contractual clauses regulating the transborder flow of personal data were adopted at the plenary meetings of the Consultative Committee of the Council of Europe's Data Protection Convention. Switzerland ratified the modernised Data Protection Convention of the Council of Europe (Convention 108+) shortly after the revised FADP came into force. Convention 108+ is expected to come into force in 2024.

The FDPIC regularly attends the two plenary meetings and the bureau meetings of the Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention ETS 108). At the plenary meeting in June 2023, the Consultative Committee adopted module one of the model contractual clauses regulating the transborder flow of personal data. This module covers data transfer from controller to controller. Module two covers data transfer from controller to processor (data importer). Module two was adopted at the plenary meeting in November 2023. Module three (the final module) is currently being fleshed out and covers data transfer from processor to processor. The FDPIC representative is involved in the drafting of these model contractual clauses, acting as a rapporteur.

The Consultative Committee also deals with data processing in connection with vote and elections as well as data processing in the context of neurosciences. All documents are already based on the modernised Convention 108 (referred to as 'C108+' or 'Convention 108+'). The Protocol amending Convention 108 was adopted by the Committee of Ministers on 18 May 2018. However, the modernised Convention will only come into force after it has been ratified by 38 Member States. The Convention is also open to states that are not members of the Council of Europe and therefore also has an effect outside of Europe. With the revised FADP, the C108+ was also implemented in Switzerland at federal level. As a result, Switzerland submitted the ratification instrument to the Secretary General of the Council of Europe on 7 September 2023 to become the 28th Member State. At the end of December, 31 states had ratified the Convention, and 15 states had signed it but not yet ratified it. Further ratifications are expected shortly, and the C108+ is expected to come into force in 2024.

EUROPE

Meeting with ICO and EDPB

The FDPIC informally discussed with the UK Information Commissioner and the chair of the European Data Protection Board (EDPB) the possibility of strengthening cooperation between the EDPB and countries outside the EU and the EEA that offer an equivalent level of data protection.

In September 2023, the FDPIC and the UK Information Commissioner (Information Commissioner's Office, ICO) met with the Chair of the European Data Protection Board (EDPB) for an informal meeting in Brussels to discuss future cooperation between these authorities. Dialogue within the official international bodies is ongoing.

Independently of this, the EU Commission organised a high-level meeting in early March 2024 bringing together the representatives of all the countries that benefit from an adequacy decision in order to promote the exchange of information and experience. The discussion focussed in particular on cooperation between the authorities in the enforcement of data protection regulations.

EUROPEAN CASE HANDLING WORKSHOP

International meeting in Switzerland

The annual European Case Handling Workshop (ECHW) was hosted by the FDPIC in Bern during the year under review. During this practical workshop, representatives of 37 data protection authorities from 27 European countries including Switzerland exchanged views on the latest technologies and the associated data protection issues. The purpose of the workshop was to analyse case law and discuss solutions to problems encountered on a daily basis. The FDPIC hosted the European Case Handling Workshop (ECHW) in Bern from 8 to 9 November 2023. Under the aegis of the Conference of European Data Protection Authorities (Spring Conference), the practical workshop provided a forum for data protection authorities to exchange views and was attended by over 80 representatives of 37 data protection authorities from 27 European countries including Switzerland.

JOINT STATEMENT

The 13 workshops were led by various DPAs. Topics discussed included current challenges in dealing with the latest technologies and open issues regarding national and cross-border data protection practices in Europe and Switzerland. These included the handling of digital facial detection (vs. facial recognition) technologies and their impact on data protection, and the definition of ‘personal data’ in the context of cutting-edge technologies such as AI and analytics and advertising tracking. Another topic discussed was the US Cloud Act and authorised access by US law enforcement authorities to personal data processed by US companies based in Europe, also in connection with projects in the public sector in which cloud applications (e.g. Microsoft 365) are used.

The lively discussions and the active participation of all present resulted in a constructive exchange and provided valuable input for the daily work of European and Swiss data protection authorities.

Joint statement on data scraping and data protection

The FDPIC has signed a joint statement, along with eleven other national data protection authorities, calling for social media platforms to protect personal data from data scraping. ‘Data scraping’ is understood as the automated extraction of data from the internet.

In August 2023, the FDPIC published a joint statement, along with eleven other national data protection authorities, calling for social media platforms to protect personal data from data scraping. ‘Data scraping’ is generally understood as the automated extraction of data from the internet.

In the statement, social media companies and website operators are urged to take action to protect personal data from data scraping. Data scraping can constitute a data breach. Under



the new FADP, which came into force on 1 September 2023, companies are required to report to the FDPIC any breach of data security that poses a high risk to the privacy or fundamental rights of data subjects (Art. 24 para. 1 FADP).

The joint statement lists the precautions individuals can take to minimise the risk of their personal data being scraped. Social media companies and website operators are required to actively provide information on how they protect their customers against data scraping and on the measures their customers can take in order to protect their own data.

INTERNATIONAL

OECD

The OECD conducts extensive research and analysis on data governance to provide a basis for international discussions. At the same time it seeks to improve trust in cross-border data flows. To this end, it fosters a global digital environment that enables the movement of data across international borders while ensuring that, upon crossing a border, data is granted the desired oversight and protection.

As a geographically diverse international organisation, with members including the US, Japan and Australia as well as European countries, the OECD plays a pioneering role in promoting privacy protection on a global level. Although most of the OECD's instruments are of a soft-law nature, they often lay the foundations for future negotiations on legally binding instruments. The OECD's work in the area of data protection is seen as a source of inspiration for important international instruments such as the GDPR and the EU-US DPF.

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 the CDEP's other working parties and other OECD bodies and develops and promotes evidence-based policies on data governance and privacy with an aim to maximise the social and economic benefits from the wider and more effective use of data while at the same time addressing the associated privacy risks and challenges. Areas of work worth mentioning in this context include the review of the OECD recommendation on cross-border cooperation in the enforcement of laws protecting privacy, new evidence and analysis of business experience with Data Free Flow with Trust (DFFT), and an analysis of current regulatory and policy approaches to emerging privacy-enhancing technologies (PETs).

SCHENGEN

BTLE and EDPB

The Border Travel and Law Enforcement (BTLE) group – a subgroup of the European Data Protection Board (EDPB) – also deals with issues related to the Schengen acquis. As a Schengen associate State, Switzerland participated in Schengen-related activities. These included developing and finalising guidelines on the application of Article 37 of the Directive (EU) 2016/680 and creating new guidelines on the rights of data subjects under the directive.

During the year under review, the BTLE subgroup developed guidelines on Article 37 of the EU Directive (EU) 2016/680 – which regulates data protection in the area of law enforcement – which it submitted to the EDPB. Article 37 of the directive ('Law Enforcement Directive (LED)' for short) regulates 'transfers subject to appropriate safeguards'. In particular, the guidelines set out the legal requirements that appropriate safeguards must meet when data is transferred to a third country (i.e. a country outside the EU/EEA). In that context, the FDPIC

SCHENGEN

pointed out that, as a Schengen associate State, Switzerland was not a third country, which was taken into account, as it was not considered as such within the meaning of Article 37. After the work was completed, the document was made available for public comment from 27 September to 8 November 2023.

Work has just begun on the development of new guidelines on the 'rights of data subjects' under the above-mentioned directive. The focus here is on Articles 12 and 15 LED ('Communication and modalities for exercising the rights of the data subject' and 'Limitations to the right of access'). Other aspects currently being examined in this context are direct access (i. e. by the controller) and indirect access (via the data protection authority, as in Belgium for example) to personal data. Explanatory notes are being prepared.

Supervision Coordination Groups on the SIS II, VIS and Eurodac information systems

Data processing in the Schengen information systems has returned to pre-Covid levels after a sharp decline during the pandemic. Some countries received a particularly large number of requests for information. For the first time, an active exchange with civil society took place via a selection of NGOs.

The SIS Coordinated Supervision Committee (CSC) and the VIS and Eurodac Supervision Coordination Groups (SCG) are bodies established under EU law to monitor the protection of personal data in the respective information systems. These groups are composed of the European Data Protection Supervisor and representatives of the national data protection authorities.

Under the new evaluation and monitoring mechanism, all Schengen Member States will in future be evaluated every seven years instead of every five. The evaluations cover data protection, police cooperation, large-scale IT systems (SIRENE, SIS), return, border protection and visa expert pools. The FDPIC sent an expert to evaluate the level of data protection in Estonia on 13–17 November 2023.

With the transfer of the secretariat from the European Data Protection Supervisor (EDPS) to the European Data Protection Board (EDPB) in March 2023, the number of annual meetings on the SIS has been increased from two to four. At the meetings, the data protection authorities noted that a particularly large number of Schengen requests for information were being received from specific countries; in some cases, the same requests were even being sent to dozens of data protection authorities at the same time. The situation is currently being monitored.

This year, civil society have been actively involved in a SIS CSC meeting, with a number of large European NGOs invited to the table.

After a sharp decline during the pandemic, data processing is now back to pre-Covid levels.

SCHENGEN

Schengen Coordination Group of the Swiss data protection authorities

The data protection authorities of the Swiss Confederation and cantons and of the Principality of Liechtenstein met twice within the framework of the Schengen Coordination Group under the chairmanship of the FDPIC.

The Schengen Coordination Group of the Swiss federal and cantonal data protection authorities met in June and December 2023 under the chairmanship of the FDPIC. The Data Protection Authority of the Principality of Liechtenstein is a member with observer

status. At both meetings, the FDPIC reported on the outcome of the meetings held in Brussels by the European Supervision Coordination Groups on the SIS and VIS information systems. The FDPIC and the cantonal data protection authorities shared the findings of their checks.

The cantons report that regular log file checks on employees with access rights to the Schengen information systems ensure greater awareness of data protection.

Now that the Coordination Group is governed by a formal federal act and no longer by just an ordinance, the rules of procedure have been formally amended.

A sub-working group is currently developing a template that the cantonal data protection authorities can use to update their websites. The aim is to make it easier for them to publish Schengen-related information, allowing data subjects to learn about their rights among other things.

SCHENGEN

Schengen-related activities at national level

The inspection at fedpol as the central access point to the Central Visa Information System (C-VIS) was continued, and a log inspection was launched at the Swiss Border Guard.

The FDPIC continued the inspection that he had started the previous year at fedpol – as the central access point to the C-VIS – relating to the retrieval of Schengen visa data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. However, the inspection was subsequently suspended following the recently launched Xplain investigation (see Section 1.2).

INTERNATIONAL MEETING

During the year under review, the FDPIC also launched a VIS log inspection at the Swiss Border Guard aimed at verifying the legality of access to the system. In order to carry out the inspection, the FDPIC asked the data protection officer of the State Secretariat for Migration (SEM) to provide a random sample of the log files of authorised Border Guard employees relating to a specified period, which he analysed. The FDPIC conducted a number of interviews with the authorised employees, during which the latter were asked to explain and substantiate the lawfulness of individual requests.

Each Schengen Member State must have a national supervisory authority established in accordance with Regulation (EU) 2016/679 to monitor the lawfulness of the processing of personal data by that country. Under Regulation (EC) No. 767/2008, Member States are required, in accordance with national law, to ensure that records of transfers from the C-VIS are kept and made available to national data protection authorities on request. In Switzerland, the competent authority for this matter is the SEM.

Association of Francophone Data Protection Authorities

[The Association of Francophone Data Protection Authorities \(AFAPDP\), of which the FDPIC is a member, met in Tangier on 2–3 October 2023.](#)

The two-day conference was attended by independent authorities from 26 countries sharing a common language, values and legal tradition.

This year's conference focused on data scraping, i.e. the automated process of extracting personal information from the Internet. This practice poses a number of risks to personal data, including targeted cyber attacks, identity theft, profiling, spamming and unauthorised direct marketing. The Office

of the Privacy Commissioner of Canada, the Moroccan data protection authority (CNDP) and Switzerland's Federal Data Protection and Information Commissioner presented the joint statement they published last August along with 11 other data protection authorities urging digital companies to take a number of measures.

The FDPIC presented Switzerland's new Federal Act on Data Protection during a round-table discussion of legislative changes and news in the field of data protection in French-speaking countries.

The AFAPDP also held its 14th Annual General Meeting, during which it examined and adopted its financial and policy reports. In addition, the Association welcomed the authorities of Georgia, Kosovo and Mauritania – member states of the Organisation internationale de la Francophonie – bringing the number of its members to 26.

INTERNATIONAL COOPERATION

Privacy Symposium in Venice

The FDPIC attended the Privacy Symposium, an international conference aimed at facilitating dialogue, cooperation and convergence among experts, researchers and data protection authorities from around the world. The 2023 edition of the Privacy Symposium took place in Venice, Italy, from 17 to 21 April under the patronage of the Italian data protection authority (the Garante).

The Privacy Symposium provided an opportunity to discuss the latest developments and prospects of data protection and privacy. Hosted by the Ca' Foscari University of Venice, it brought together more than 200 top-level speakers in more than 80 sessions on a variety of thematic tracks including international cooperation, technology and compliance, socio-economic perspective and research and innovation.

The opening day was devoted to a special programme on the Council of Europe's privacy and data protection treaty (Convention 108), with several sessions and workshops addressing the future impact of the protocol modern-

ising the treaty (Convention 108+) in achieving stronger data protection globally and an easier data flow among countries.

The FDPIC presented the new Federal Act on Data Protection, his role in Convention 108 and the promotion of cooperation between and with European supervisory authorities that are not EDPB members.

He also held informal discussions with his Italian and German counterparts (Garante and BfDI respectively), as well as with the European Data Protection Supervisor, on subjects such as ChatGPT, cloud computing and cross-border data flows.

GLOBAL ISSUES

Global Privacy Assembly

The Global Privacy Assembly shone a spotlight on new technologies and their impact on privacy. At its annual meeting, it adopted seven resolutions, including two on artificial intelligence.

The purpose of the Global Privacy Assembly (GPA) is to discuss key privacy issues and how regulators can work effectively – both individually and collectively – to protect privacy in an increasingly data-driven world.

The privacy impacts of technologies such as artificial intelligence (AI) and generative AI were an important focus of the annual meeting, which adopted two resolutions on the subject:

- One on generative artificial intelligence systems, calling on those who develop, deploy and operate these systems to adhere to the key principles of data protection and privacy;
- The other on artificial intelligence in the employment context, highlighting the importance of data protection and privacy principles and safeguards in the development and use of artificial intelligence systems in employment (including recruitment).

At the meeting, the GPA also adopted the following five resolutions:

- A resolution on global data protection principles aimed at updating the principles adopted by the GPA in Madrid in 2009 in the light of recent technological developments. The resolution includes new principles such as privacy by design and by default, the right to data portability, and a framework for profiling and automated decision-making;
- A resolution on the creation of a library of resources on the key principles of data protection;
- A resolution on the creation of a working group on an intersectional gender approach to data protection;
- A resolution on health data and scientific research;
- A resolution proposing a joint GPA/ Access Now prize on data protection and human rights.

Finally, the Assembly also adopted its Strategic Plan 2023–2025, which focuses on areas of strategic interest for the GPA including the rights of data subjects and enhancing the capacity of data protection authorities.

The Global Privacy Assembly, of which the FDPIC is a member, was established in 1979. Its 45th annual meeting was held in Hamilton, Bermuda, from 15 to 20 October 2023.

INTERNATIONAL

European Conference of Data Protection Commissioners in Budapest

The European Conference of Data Protection Commissioners discussed the latest developments and outstanding issues regarding cross-border data flows. Other topics included cooperation between data protection authorities – examples of which were presented – and ways of raising public awareness of the importance of data protection. An open session was held for the first time. The closed session of the European Conference of Data Protection Commissioners focused on four topics: new technologies, competition law, court decisions and best practices/case studies in enforcement cooperation between EEA and non-EEA countries. The panel on new technologies examined the impact of technology on our society, in particular on our thinking and our human relationships; The panel on competition law explored the interlinkages between competition law and data protection with a view to identifying how these two areas of law can support each other; The panel on best practices/case studies in cooperation between EEA and non-EEA countries gave an overview of the experience gained in cooperation between countries outside the GDPR framework; Finally, the panel on court decisions provided an update on the most important cases in Strasbourg and Luxembourg.

For the first time, the Spring Conference included a session open to the general public. The various panels explored the following themes: cooperation between data protection officers (DPOs) and data protection authorities (DPAs), DPO networks and the training of DPOs, and the DPO's role within the organisation.

The members adopted three resolutions:

- A resolution on the need for enhanced cooperation in the field of data protection and competition law;
- A resolution on the accreditation of the San Marino Data Protection Authority;
- A resolution on the revision of the rules and procedures of the Conference.

The 31st European Conference of Data Protection Commissioners was held in Budapest from 10 to 12 May 2023. The closed session was attended by 138 members of data protection authorities, while the open session was attended by more than 350 people from 39 countries.



Freedom of Information

2.1 General

The Freedom of Information Act (FoIA) seeks to promote transparency with regard to the mandate, organisation and activities of the Administration by ensuring access to official documents (see Art. 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 requests received in 2023 for access to official documents indicate that the media and society's need for specific information and transparent Administration (including administrative behaviour) is as strong as ever, with applications for access reaching an all-time high. During the year under review, the number of applications received by the federal authorities was almost 50 %

higher than the previous year. According to the authorities, the amount of time required to process the applications has increased accordingly. Overall, implementing the principle of freedom of information has again proved to be a demanding and challenging task. The figures in Section 2.2 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 do not agree with the authorities' decision to

grant access, the Freedom of Information Act entitles them to submit a request for mediation to the FDPIC. The FDPIC received 132 mediation requests during the year under review, namely 2 % more than the previous year. The purpose of mediation is to enable a swift agreement between the parties. Oral mediation sessions proved beneficial again in 2023: An analysis of the mediation requests processed in the year under review shows that where a mediation session was held, an amicable solution was reached in 55 % of cases.

The consistently large number of mediation requests in recent years and the large number of mediation procedures that had to be conducted by correspondence due to the pandemic have created a backlog in the completion of procedures. At the same time, the

complexity of enquiries and the associated legal issues is increasing. Cases in point during the year under review include the mediation procedures relating to the Covid-19 vaccine contracts and the takeover of Credit Suisse by UBS. As a result, the FDPIC exceeded the statutory processing time of 30 days again during the year under review in a large number of cases.

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 (see Section 2.4). In this context, the Administration

regularly argues that compliance with statutory reporting and cooperation obligations can only be guaranteed if the Freedom of Information Act is excluded. In the FDPIC's view, however, in a state governed by the rule of law, statutory information and reporting obligations can be expected to be observed and enforced. Any potential violations by supervised entities – even if or precisely because they relate to the principle of freedom of information – can in no way justify restrictions of this kind to the Freedom of Information Act. Reservations of this sort undermine the principle of freedom of information and the transparency within the Administration that the principle seeks to achieve. An overview of special reservations under Article 4 FoIA can be found in Section 2.5.

2.2 Applications for access: sharp rise in 2023

According to the figures released, the federal authorities received 1701 applications for access to information during the year under review, i. e. 48% more than in 2022 (1153). In 2023, they also processed 37 applications for access that had been submitted in previous years. They granted full access in 830 cases (48%), compared with 624 (53%) in 2022. In 402 cases (23%), access to the documents was partially granted or deferred, compared with 236 cases (20%) the year before. In 176 cases (10%), access was fully denied, compared with 99 cases (8%) in 2022. According to the authorities, 73 applications were withdrawn (4%) (compared with 53 (5%) in 2022), 96 applications were still pending at the end of 2023, and in 161 cases there was no official document.

The number of applications for access to documents of the Administration is likely to remain high in the coming years, even though the need for information and transparency – which was particularly strong during the Covid-19 pandemic – shifted focus to other global events during the year under review. The authorities produced statistics on applications for access to documents relating to Covid-19, which it sent to the FDPIC along with the

data to be reported annually (see statistics on applications for access to Covid-19 documents). According to the federal authorities, 39 out of 1738 applications for access processed (2%) were for documents relating to Covid-19, again considerably fewer than the previous year (8%). Access was granted in full in 12 cases (31%), i. e. less frequently compared with the overall statistics. The authorities granted partial access or deferred access in 17 cases (44%), therefore more frequently in relation to Covid-19 documents, while access was denied completely in 1 case (2%, i. e. five times less frequently compared with the overall statistics). Two applications for access to Covid-19 documents were still pending at the end of 2023, and in seven cases there was no official document.

In summary, the FDPIC notes that, during the year under review, for the first time since 2015, full access to the documents was granted in less than 50% of cases. By contrast, the number

of applications for access fully denied remains low, having stabilised at just under 10% in recent years.

Federal departments and federal offices

Several administrative units were the focus of much media and public interest in 2023. Due to the nature of their work, the DDPS (432), DETEC (236), FDHA (230) and FDFA (228) received large numbers of applications for access. In the case of the FDHA, 15% of the requests received by all offices concerned official Covid-19 documents, compared with 38% the previous year. The authorities in question reported that the applications received were sometimes very extensive and complex, many of them requiring lengthy coordination between federal offices and departments.

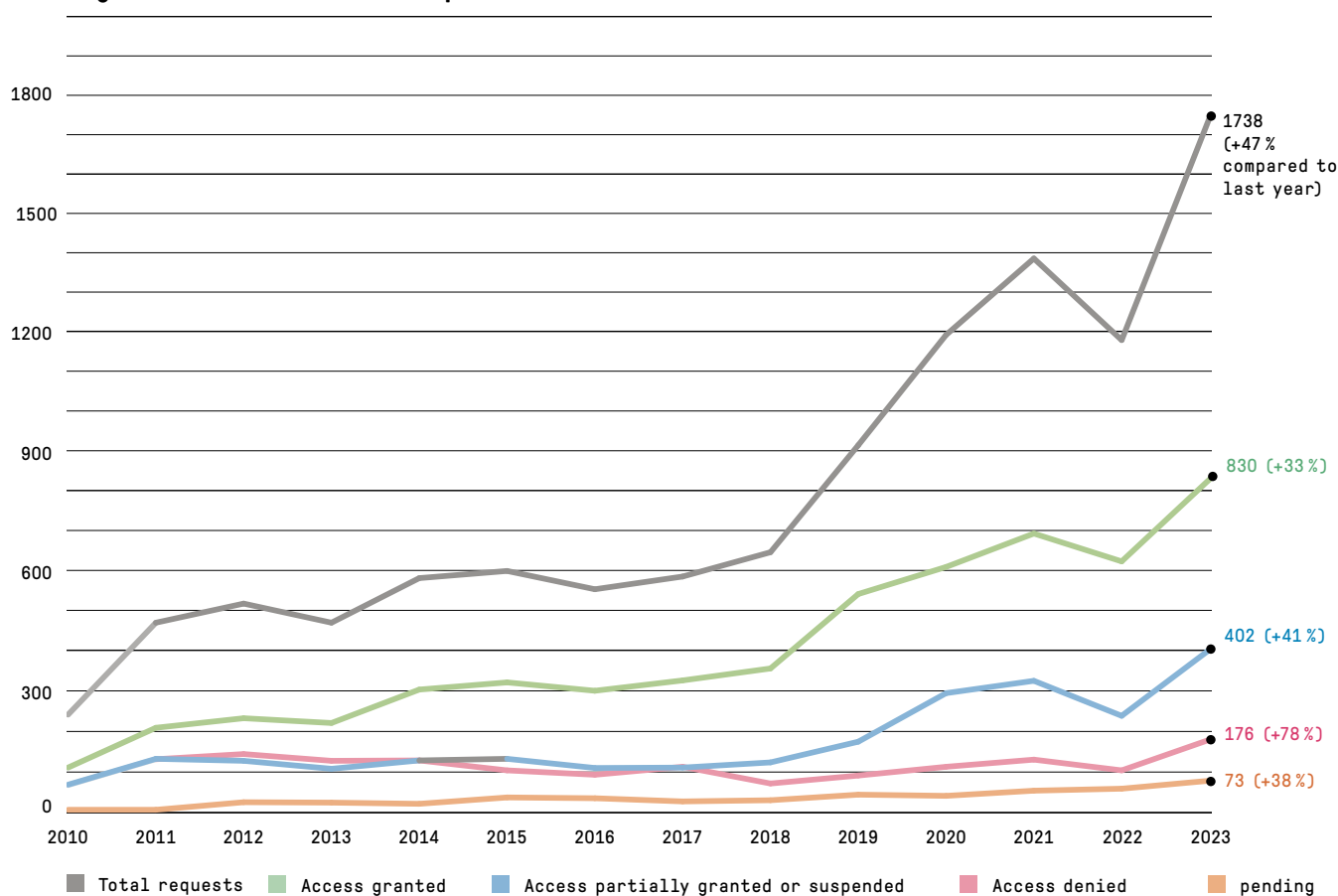
The figures released by the federal offices indicate that the FOSPO received the most applications for access in 2023, namely 277, followed by the FOEN with 98, the GS-FDF with 87 and the GS-DDPS with 83. Fourteen authorities reported receiving no applications for access during the year under review. The FDPIC himself received 14 applications for access and granted full access in ten cases; access was fully denied in one case, and three cases were still pending at the end of 2023.

In 2023, fees charged for access to official documents totalled CHF 14,226, 42 % less than the previous year (CHF 24,582). While 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 and the Federal Chancellery did invoice applicants for some of the time spent dealing with their applications for access (FDHA: CHF 6,403; EAER: CHF 4,498; DETEC: CHF 1,675; FDF: CHF 1,500; Federal Chancellery:

CHF 150). It should be noted that just 19 out of 1738 applications for access processed incurred a fee. Compared with the previous year, when fees were charged in 29 cases, both the number of cases in which a fee was charged and the total amount charged were significantly lower this reporting year. Fee-charging remains the exception, with applications for access incurring no fee

in just under 99 % of cases in 2023. Observed again in the year under review, the administrative practice of granting free access to official documents was enshrined in the Freedom of Information Act on 1 November 2023. By way of exception, the authorities may continue to charge fees for applications for access that requires disproportionate effort to process. The Federal Council has defined that more than eight working hours are deemed as disproportionate effort, whereby the FDPIC had pointed out that setting the time

Figure 1: Evaluation of requests for access – trend since 2010





threshold too low would not reflect the legislator's intention (see Section 2.4 on the corresponding amendment to the Freedom of Information Ordinance).

The FDPIC points out that the authorities are under no obligation to record the time they spend processing applications for access and that there are no legal requirements for 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 for access. According to the data received, processing time during the year under review stands at 6,469 hours, significantly more than the previous year (5,404 hours).

The fact that the time spent processing applications for access reported by the authorities reflects only a portion of the time actually spent is illustrated, for example, by the data provided by the FOPH. In addition to the 287.5 working hours reported by the FOPH's specialist units and the legal support provided by its freedom of information advisor amounting to 80 % full-time equivalents (FTEs), the FOPH again reported a large amount of time (amounting to at least 2.8 FTEs) spent processing applications for access to

Covid-19 related documents (including mediation requests and appeal procedures). The same applies to other units of the Federal Administration.

The amount of time spent preparing mediation procedures has decreased to 730 hours, compared with 1006 hours the previous year, 865 hours in 2021, 569 hours in 2020, 473 hours in 2019, 672 hours in 2018, and 914 hours in 2017.

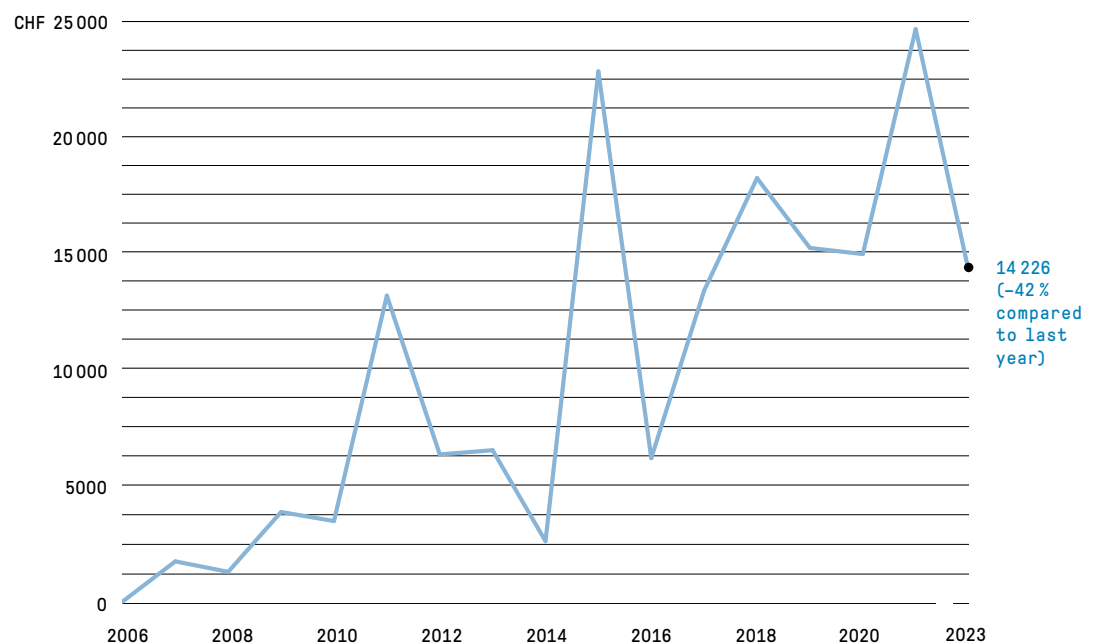
Parliamentary services

The Parliamentary services reported receiving two applications for access during the year under review. Access was fully denied in one case, and in the other case there was no official document.

Office of the Attorney General of Switzerland

The Office of the Attorney General of Switzerland reported receiving two information requests in 2023. Access was granted in full in one case, and in the other case there was no official document.

Figure 2: Fees charged since the FoIA entered into force



2.3 Mediation procedures: slight increase in mediation requests

In 2023, the FDPIC received 132 mediation requests, 2% more than in 2022 (129 requests). The majority of mediation requests was filed by the media (74) and private individuals (31). According to the figures, of the 739 cases in which the Federal Administration fully or partially denied access, deferred access or stated that there were no official documents, 132 cases (18% of cases) resulted in a mediation request being filed.

In 2023, 142 mediation requests were settled, 18 (14%) of which concerned official Covid19-related documents; 105 of the requests had been filed during the year under review, 34 the previous year, and 3 in previous

years. In 54 cases, the participants were able to reach an agreement. The FDPIC issued 47 recommendations, enabling him to settle 61 cases which were unlikely to result in an agreement between the parties.

The cases dealt with include 12 requests which had not been filed on time, nine cases which did not satisfy the conditions for application of the Freedom of Information Act, and six mediation requests that were withdrawn.

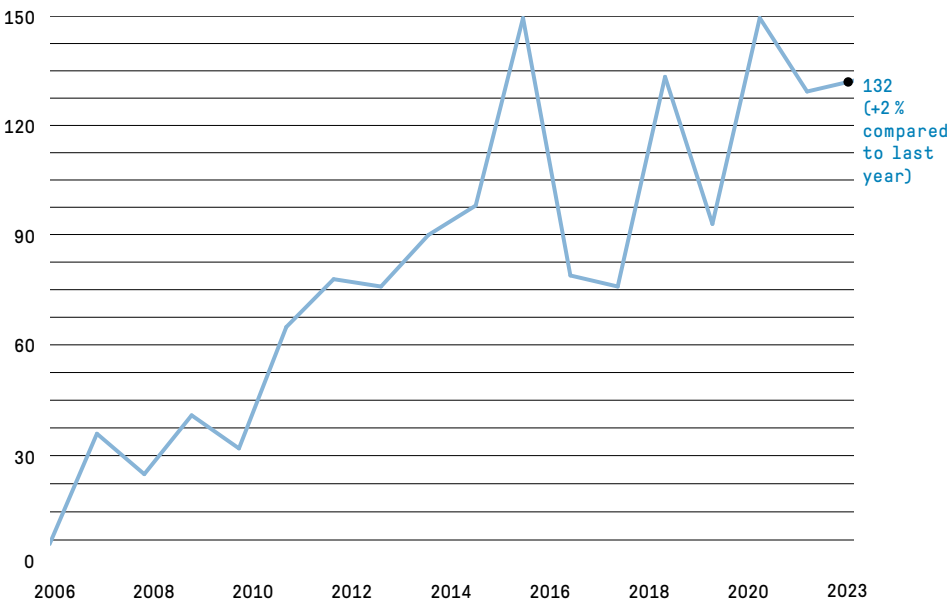
At the end of the year, nine mediation procedures had been suspended by agreement between the participants or at the applicants' request.

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 of the mediation session.

The ratio of amicable outcomes to recommendations is the best measure of the effectiveness of oral mediation sessions. During the year under review, 54 amicable outcomes were

Figure 3: Mediation requests since the FoIA entered into force



achieved, and the FDPIC issued 47 recommendations to settle 61 cases. Therefore, the ratio of amicable outcomes to recommendations is 47%. However, this needs to be explained: amicable solutions are often only reached when mediation sessions take place. In the 62 mediation sessions that took place during the year under review, an agreement was reached in 34 cases (55%). In the 58 cases in which face-to-face mediation sessions with the parties could not take place (for example because of the large number of participants), an agreement was reached in only 20 cases (34%).

Therefore, we can conclude that oral mediation sessions continue to be effective in reaching amicable solutions. In the FDPIC's view, this method should therefore continue to be favoured over mediation by correspondence and promoted accordingly. Oral mediation sessions prove beneficial for all parties involved in the mediation procedure.

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

Table 1: Amicable outcomes

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

Duration of mediation procedures

The table below is divided into three sections according to processing time. It should be noted that the processing time indicated does not include the period during which a mediation procedure is suspended at the participants' request or with their consent. A mediation procedure is typically suspended when an authority wishes to review its position after the mediation session or has to consult the third parties involved. 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 between the originally scheduled date and the rescheduled date or the period of time by which the proceedings are extended.

The table shows that 27% of mediation procedures completed in 2023 were concluded within the 30-day period, while 35% took between 31 and 99 days, and 38% took 100 days or more.

Of the 39 mediation requests settled within the 30-day period, only 15 (38%) mediation procedures were settled by agreement or with a recommendation following a discourse of the issues that were the subject of mediation. In the other 24 cases (62%), 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 procedures took longer again during the year under review because of the processing backlog from previous years. In addition, the number of mediation requests received is typically subject to fluctuation. For example, the FDPIC received a large number of requests in April (15), November (15) and March (17) but just five in September and two in August.

The statutory 30-day deadline for completing the mediation procedure was regularly met before the pandemic when the mediation sessions culmi-

nated in agreement. Although this was not the case in the year under review, the proportion was slightly higher than the previous year: When the mediation sessions culminated in agreement, the 30-day deadline was met in 35% of cases compared with 29% the previous year. The backlog and the limited human resources available for processing the mediation requests meant that in 83% of cases it was already 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, only in one case did he manage to do so within the statutory period of 30 days from receipt of the mediation request.

Failure to meet the deadline was often due to particularly extensive application for access, the large number of third parties involved in the procedure, or complex legal issues. These explanations also apply to the 54 cases that took 100 days or longer to process. These include, for example, the mediation procedures relating to the Covid-19 vaccine contracts and the takeover of Credit Suisse by UBS (see the FDPIC's recommendations of 23 and 27 November 2023). 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

Tabelle 2: Processing time of mediation procedures

Processing time in days	2014 – August 2016*	Pilot phase 2017	2018	2019	2020	2021	2022	2023
within 30 days	11%	59%	50%	57%	43%	42%	25%	27%
between 31 and 99 days	45%	37%	50%	38%	30%	51%	42%	35%
100 days or more	44%	4%	0%	5%	27%	7%	33%	38%

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

(FoIO; RS 152.31) – the FDPIC may extend the deadline by an appropriate period of time.

On a positive note, in contrast to the two previous years, more mediation requests were processed in 2023 (142) than were received (132).

Number of pending cases

The figures below indicate the number of pending cases at the end of the reporting years shown. At the beginning of January 2024, 31 mediation procedures were still pending, including

nine suspended procedures (one from 2019, one from 2021, two from 2022, and five from the year under review).

17 cases had been completed by the time of going to press.

Table 3: Pending mediation procedures

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 (13 completed in February 2019 and 2 suspended)

2.4 Legislative process

FINANCE

Credit Suisse: Emergency ordinance incorporated into the Banking Act

The UBS takeover of Credit Suisse was carried out under emergency legislation enacted by the Federal Council, which provided that related official documents were excluded from access under the Freedom of Information Act. In the subsequent ordinary legislative procedure, the FDPIC opposed the inclusion of such a provision.

In view of the severe market turbulence with which Credit Suisse was struggling, on 16 March 2023 the Federal Council issued a temporary ordinance (Ordinance on Additional Liquidity Assistance Loans and the Granting of Federal Default Guarantees for Liquidity Assistance Loans from the Swiss National Bank to Systemically Important Banks) based directly on the Federal Constitution. On this basis, it adopted a package of measures to stabilise the Swiss economy, which enabled the takeover of Credit Suisse by UBS and included guarantees from the Confederation and the SNB totalling CHF 209 billion. The emergency ordinance excludes citizens' rights of access under the Freedom of Information Act to information and data relating to enforcement of said ordinance. The

explanatory notes declared this a special provision that took precedence over the Freedom of Information Act.

In the consultation draft on the amendment of the Banking Act, the State Secretariat for International Finance (SIF) proposed that the exclusion of the Freedom of Information Act continue after the emergency package had been incorporated into ordinary federal law. To justify the continued exclusion, the SIF argued that the information and data made available was of a sensitive nature and may often contain business or manufacturing secrets within the meaning of the Freedom of Information Act. In addition, the SIF believed that excluding the Freedom of Information Act would ensure that the financial institutions concerned would provide the competent administrative units with all the information needed in order to implement the ordinance in a timely manner. Based on the same argument,

the SIF intended to restrict the Freedom of Information Act further by excluding information relating to the granting of default guarantees for transactions under the Mergers Act. The FDPIC opposed all proposed restrictions to the Freedom of Information Act and, in addition to raising objections based on intertemporal law, argued that denying the public access to documents relating to the granting of financial aid – as was the case with the Covid-19 Loan Guarantees Act (see 28th Annual Report, Section 2.4) and «rescue umbrella» for the electricity industry (see 30th Annual Report, Section 2.4) – would further undermine the very purpose of the Freedom of Information Act.

The Federal Council removed the two restrictions from the consultation draft, as requested by the FDPIC. The draft amendment to the Banking Act that is currently being discussed by the competent committees of the Federal Parliament no longer contains the contested exceptions to freedom of information.

More detailed information on the exclusion of documents from the Freedom of Information Act under the emergency ordinance can be found in the FDPIC's recommendations of 27 November 2023.

ARCHIVING

Partial revision of the Archiving Ordinance

The Federal Archives would like to see the Archiving Ordinance amended in order to coordinate the Archiving Act and the Freedom of Information Act and to clarify which of the two acts applies when access is requested under the Freedom of Information Act to archived documents during the retention period. Instead, the FDPIC is calling for the Archiving Act to be amended.

Back in 2022, during the office consultation on the discussion document regarding the need to revise the Archiving Act, the FDPIC had already pointed out the extensive practical consequences of coordinating the Archiving Act and the Freedom of Information Act and regulating which of the two acts applied to applications for access to archived documents during the retention period. Accordingly, we had called for coordination of the two federal acts to be regulated at the legislative level (see 30th Annual Report, Section 2.4).

The Federal Archives initially discarded the request as premature. Subsequently, after taking on board the FDPIC's opposing view, the Federal Council decided that coordination should be regulated with an amendment to the Archiving Ordinance.

The Federal Archives' revised rules introduced the principle of 'application of the more favourable act', meaning that when a request is examined, the more favourable of the two access regimes (Archiving Act or Freedom of Information Act) would be applied depending on the case at hand. The Federal Archives wanted to see this coordination rule enshrined in the Archiving Ordinance.

In the preliminary consultation, the FDPIC pointed out that assessing a request and determining the more favourable legal basis on a case-by-case basis was at times difficult or even impossible. The formal and substantive requirements of the Freedom of Information Act and the Archiving Act differ significantly, making a comparison very difficult. The preliminary draft also failed to specify whether it was up to the applicant or the authority to decide which of the two acts was more favourable and would therefore apply to the procedure up to this decision. Finally, the wording of the proposed provision implied a merely alternative application of the two acts, meaning that a request would be assessed based exclusively on either the Freedom of Information Act or the Archiving Act, supposedly restricting one of the two.

The FDPIC questioned whether, under an ordinance provision, an applicant could be denied the right to have a negative decision by the authority reviewed in an appeal under both the Freedom of Information Act and the Archiving Act (corresponding the respective appeal proceedings). He concluded that the ordinance provision proposed by the Federal Archives would not be practicable and was no substitute for coordinating the Archiving Act and the Freedom of Information Act at the legislative level.

In the draft for a partial revision of the Archiving Ordinance that was submitted for office consultation, the Federal Archives opted not to regulate coordination. Instead, it was decided to continue with the current practice and to gather information on practicality and cost. The Federal Archives motivated their decision based on feedback from the FDPIC among others despite the fact that, as we explained in the office consultation, continuing the current practice cannot be regarded as a suitable solution in terms of coordination as it has revealed many aspects of a formal and substantive nature that have yet to be clarified.

New federal act on the transparency of legal entities

Under new legislation on the transparency of legal entities, a central register shall be set up listing the actual beneficial owners of legal entities. Despite the FDPIC's intervention, the draft bill provides for the exclusion of the Freedom of Information Act.

On 30 August 2023, the Federal Council began the consultation procedure for the new Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners (LETA). The Act provides for the introduction of a federal 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.

The preliminary draft of the State Secretariat for International Finance (SIF) regulates which authorities and persons may access the new register of beneficial owners. In the explanatory report, the SIF states that (unlisted) third parties shall not have access to the information as, given the limited public interest, extending access to the register would constitute a disproportionate interference with the constitutional right to privacy and protection of personal data against misuse. The original explanatory report also states that the access rules constitute special provisions within the meaning of Art. 4 let. b of the Freedom of Information Act. The reservation of special provisions means that the Freedom of Information Act does not apply to access to this information.

During the consultation, the FDPIC stated that, in his view, the provisions in question could not be regarded as special provisions. Instead, the Act regulated the right of access to the register and the associated disclosure of data and therefore merely created a legal basis for the disclosure of data within the meaning of Art. 36 FADP/ Art. 57r GAOA. In the FDPIC's view, any comment in the explanatory

report did not change this. Regardless, the FDPIC sees no need to deny access to the data in the register altogether and unconditionally under the Freedom of Information Act, especially since the exemption clauses enshrined therein explicitly guarantee comprehensive protection of the private interests of data subjects.

In the explanatory report on the consultation draft, the wording according to which the access rules constitute special provisions in accordance with Art. 4 of the Federal Act on Freedom of Information was finally dropped. To the regret of the FDPIC, however, following the consultation procedure, the Federal Council then supplemented the draft law with an explicit exclusion of the Freedom of Information Act, according to which it does not apply to data from the transparency register that relates to natural and legal persons. (see also Section 1.3)

FEES

Free of charge as a principle: fees charged only for applications that take particularly extensive processing

Parliament has adopted the principle of free access to official documents and has decided that authorities may only charge a fee for applications for access that take particularly extensive processing. The Federal Council has defined that more than eight working hours are deemed as extensive processing. The FDPIC had argued in favour of a higher fee-charging threshold.

In September 2022, Parliament had decided that access to official documents should be free of charge as a matter of principle instead of the previous principle of charging fees. By way of exception, authorities may charge fees for applications for access that require particularly extensive processing. The legislator instructed the Federal Council to regulate, in the Freedom of Information Ordinance, the number of working hours beyond which processing would be considered particularly extensive and may therefore be subject to a fee. In addition, the Federal Council was asked to set an hourly fee rate for processing time above the fee-charging threshold. That way, in the exceptional cases in which fees were charged, these would be based on an objective criterion, namely extensive

processing time spent, thus preventing inconsistent fee-charging practices across the Federal Administration.

In a preliminary consultation in the interdepartmental working group ‘Transparency’ and in the subsequent office consultation on the amendment of the Freedom of Information Ordinance, the FOJ had proposed – in addition to editorial changes – a threshold of 30 working hours, beyond which processing would be considered particularly extensive. The FDPIC pointed out that, by introducing the principle of access free of charge, the legislator intended to minimise disputes over fees and promote free access to information of the Administration and considered the legislative amendment to be a decisive step towards strengthening freedom of information. The FDPIC considered the 30-hour threshold reasonable. With regard to any calls for a lower threshold, he stressed that any solution implemented by the

Federal Council had to reflect the intention of the legislator and that reducing the fee-charging threshold should therefore not result in an increased burden on applicants, authorities and courts, effectively achieving the opposite of what was intended with the revision.

In response to the opinions voiced during the office consultation, the FOJ lowered the threshold from 30 to 20 hours. The FDPIC went on to point out that, in his view, this lowering of the threshold did not reflect the intention of the legislator.

In September 2023, the Federal Council decided to lower the fee-charging threshold to as little as eight working hours. Above this threshold, individuals applying for access can therefore be charged CHF 100 per hour of work. Applicants must be informed in advance if a fee is going to be charged.

The fee for applications for access made by a journalist shall be reduced by 50 %. Furthermore, the Federal Council has decided that authorities must report annually to the FDPIC the number of cases in which a fee was charged as well as the total amount of fees charged for access to official documents. The new legislation came into force on 1 November 2023.

Opinion of the Federal Council

In its investigation 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) states that the rules for filing and archiving documents in the Federal Administration are not uniform and need to be clarified. The Committee also concludes that the FDPIC's inspection rights should be strengthened. In its view, the Federal Council should examine the possibility of granting the FDPIC a right of intervention or a right of disposal in the Freedom of Information Act in the event that his inspection rights are not respected. The Federal Council rejects a right of disposal but is willing to consider rights of intervention.

In a newspaper article of 14 June 2022, it was reported that, in connection with an attempt to blackmail Federal Councillor Alain Berset, a number of emails had been lost or deleted in the General Secretariat of the FDHA (GS-FDHA) and that this matter was the subject of a mediation procedure with the FDPIC. The Control Committee of the Council of States (CC-S) instructed its FDJP/FCh subcommittee to clarify – in general and with regard to the specific case at hand – the requirements regarding the filing and

archiving of documents within the Federal Administration and to specify which documents were to be made accessible under the Freedom of Information Act.

In its investigation report on the archiving and filing of documents and the procedure for applications for access according to FoIA, in which it investigates the general requirements and the specific allegation of untraceable emails within the GS-FDHA, the CC-S begins by examining the legal bases for the retention, filing and archiving of documents (in particular the Archiving Act) and access to official documents (Freedom of Information Act). It notes that the legal bases differ not only in terms of terminology, but also in terms of objectives, subject matter and scope and therefore require clarification.

With regard to the specific case at hand, the Committee states that it could not be definitively established whether the untraceable emails existed, how many there were or

whether any of them may have been deleted. However, it seems safe to assume that the emails in question would not have been strictly personal but would also have been work-related.

In its report, the CC-S clearly states that the retention and archiving of documents and the granting of access to official documents of the Federal Administration are essential for transparency and traceability of the Administration's actions. The CC-S also states that the GS-FDHA has failed to fulfil its legal obligations under the Freedom of Information Act by denying the FDPIC access to documents within the context of mediation procedure. In the report, the Committee points out that the FDPIC's right of inspection (under the Freedom of Information Act) in a mediation procedure is crucial in order to assess whether documents or emails are to be considered official documents. If access is denied by the authorities, the FDPIC is unable to properly fulfil his statutory mediation mandate. In the Committee's view, the FDPIC therefore needs to be granted access to all documents so that he is able to determine whether the documents and records are of an official nature. The Committee considers it unacceptable that the FDPIC be denied access to the disputed documents in a mediation procedure and expressly asks the Federal Council to consider amending the Freedom of Information Act to grant the FDPIC a right of intervention or a right of disposal.

The report published by the CC-S in October 2023 contains five recommendations addressed 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 person's office that also contain information relating to their private life, particularly with regard to senior members of government or of the judiciary.
- 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 of disposal in the event that his right of inspection is not respected.

The CC-S asked the Federal Council to comment on its report. The Federal Office of Justice (FOJ) held an office consultation on the Federal Council's response to the CC-S report. In its draft response, the Federal Council declares that it will fully comply with Recommendations 1–4 but will only partly comply with Recommendation 5.

Regarding Recommendation 5, it was proposed that the Federal Council should only agree to consider granting the FDPIC a right of intervention in the event that his right of inspection is not respected but a right of disposal was rejected. It was argued that, under the Freedom of Information Act, the mediation procedure was an informal, non-prejudicial procedure and that it would therefore not be according to system for the FDPIC to have power of disposal. The FDPIC argued that it was the express wish of the CC-S to consider granting him a right of intervention and, at the same time, to consider a specific right of disposal for the FDPIC instead of ruling it out right away with a pre-emptive reply. Ruling it out from the start would preclude an open review as requested by the CC-S. Therefore, the FDPIC requested that Recommendation 5 be accepted unconditionally.

The FOJ rejected the request and adhered to its opinion that the Federal Council should accept Recommendation 5 only in part: This proposal was confirmed during the office consultation, with the other participants agreeing with the FOJ's proposal or even requesting that Recommendation 5 be rejected altogether.

In its statement of 11 January 2024 to the CC-S, the Federal Council refused to consider granting the FDPIC a right of disposal. It accepted the other recommendations of the CC-S in full. Furthermore, the Federal Council instructed the FDJP to review the recommendations by the end of 2024 and to submit proposals for further action.

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 (letter a) or declare the access to certain information to be subject to requirements derogating from those set out in the FoIA (letter 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 on the amendment of the Federal Health Insurance Act (Cost containment measures – Package 2)	832.10	Art. 52c para. 1 and 2 HIA (draft) Art. 52d para. 4 HIA (draft) Transitional provision III, para. 5 HIA (draft)	Dispatch dated 7 September 2022 (Status: consultation in Parliament)
	831.20	Art. 14quinquies para. 3 IVG (draft) Transitional provision IVG (draft)	
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
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		

Legislation (short form) and abbreviation	SR no.	Art./Para.	Entry into force:
Entry into force of the Freedom of Information Act			1. July 2006
Parliament Act (ParIA)	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

(Non-exhaustive list)

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 and 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

(Non-exhaustive list)

The FDPIC

3.1 Duties and resources

Services and resources in the field of data protection

Number of staff

Regarding the additional posts allocated by the Federal Council in its dispatch on the complete revision of the FADP, as mentioned in our last annual report, the FDPIC managed to recruit and train the extra staff in good time before the new FADP came into force on 1 September 2023 (see 30th Annual Report, Section 3.1). The number of staff employed for data protection issues therefore remains unchanged at 33 full-time positions.

Table 4: Staff positions available for FADP issues

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	27
2023	33
2024	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 2023 to 31 March 2024, the FDPIC's staff resources available for data protection were allocated to these groups as follows:

Table 5: Services in data protection

Consultancy - Federal Administration	15.7	
Consultancy - private individuals	20,8%	
Cooperation with foreign authorities	15,9%	
Cooperation with cantons	0,9%	
Total consultancy		53,3%
Supervision	15,5%	
Certification	0,0%	
Data collection register	0,2%	
Total supervision		15.7
Information	14,4%	
Training, talks and presentations	3,4%	
Total Information		17,8%
Legislation	13,2%	
Total legislation		13,2%
Total data protection		100,0%

Consultancy

The FDPIC faces a consistently high demand for consultancy services as he is legally required to support large digital projects. During the year under review, the proportion of staff working in consultancy amounted to 53.3%, marginally higher than last year (52.5%). At the end of the year under review, ten large projects were receiving supervisory support in the form of consultancy. Four of these projects are related to the digital transformation of the Federal Administration. The number of enquiries and reports increased by almost 1000 compared with the previous reporting period (from 4091 to 5074). The three teams of the Data Protection Directorate responded to an average of 51 enquiries and complaints from members of the public each month with a standard letter.

Digital data processing and the use of artificial intelligence (AI) are advancing at a rapid pace in businesses and within the federal authorities, with an increase in the number of large-scale data-processing projects.

Table 6: Consultancy for large-scale projects in 2023

Fundamental rights	1
Legislation - new FADP	4
Mobility	1
Health	2
Police and Justice	2
Total	10

Supervision

The dynamics of cloud- and AI-based applications mean that inspections have to be carried out quickly. Frequent changes to programmes and terms of use and the need to combine legal and technical expertise mean that, as far as possible, the FDPIC needs to avoid long interruptions to investigations by employing more staff to manage more thorough inspections. During the year under review, 15.7 % of resources were allocated to inspections and supervisory duties – in line with the low average for the reporting years

from 2015 onwards – and 12 more thorough inspections were carried out with these resources.

The extra staff initially recruited mainly to prepare for the introduction of the new legislation will be redeployed primarily to supervisory roles. The FDPIC plans to gradually increase the frequency of inspections of federal bodies, large and medium-sized companies (around 12 000) and foundations and associations (around 10 000) across Switzerland.

Legislation

The changes in the way personal data is processed in connection with the digital transformation of the federal offices require a legal framework. This entails a large number of new and revised provisions on data processing

in federal law, on which the FDPIC is called to express his views in various consultation procedures. During the year under review, we were called on to participate in 297 office consultations.

Information

Extensive preparatory work and internal and external training were carried out in view of the entry into force of the new FADP and the implementing ordinance. Nevertheless, the proportion of resources used for the ‘Information’ service group was reduced significantly in the reporting year to 17.8 % (from 22.2 % the previous year).

Participation in committee consultations and parliamentary committee hearings

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

- April 2023: FC-S and FC-N subcommittees on the financial statements for 2022;
- April 2023: PIC-N on exclusion of the Freedom of Information Act under emergency law;
- April 2023: PIC-N on the Bendahan parliamentary initiative;
- April 2023: LAK-N on the impact of the EU Commission’s legislative proposal regarding Chat Control;

- May 2023: PIC-N on exclusion of the Freedom of Information Act under emergency law;
- May and November 2023: PIC-N on the introduction of the right to digital integrity in the Federal Constitution;
- May 2023: EATC-N on the Customs Act;
- July, October and November 2023: PIC-S on the Federal Act on the National System for the Retrieval of Addresses of Natural Persons (National Address Service Act);
- October 2023: PIC-S on the Federal Act on Health Insurance; Amendment (cost-containing measures – Package 2);
- October 2023: FC-S and FC-N sub-committees on the 2024 budget;
- November 2023: Judiciary committee;
- January 2024: PIC-N on the Federal Act on the National System for the Retrieval of Addresses of Natural Persons (National Address Service Act);
- January and February 2024: LAC-N on the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (e-ID Act);
- March 2024: LAC-S on the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (e-ID Act).

Services and resources in the field of freedom of information

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

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

Table 9: Outcome objectives for FDPIC

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.

DPO AND ITS0

FDPIC improves self-regulation

With the entry into force of the new Federal Act on Data Protection, the FDPIC has strengthened self-regulation in order to ensure that the legally compliant implementation of data protection regulations under federal law is guaranteed within his office. He has done so by creating two new part-time positions in the form of a data protection officer (DPO) and an IT security officer (ITS0).

The purpose of self-regulation is to ensure, by means of suitable control measures, that the legally compliant implementation of data protection regulations under federal law is guaranteed within our office. This task was already carried out before the revised FADP came into force but has now been formally assigned to two professionally independent officers within our authority, namely a data protection officer and an IT security officer.

The FDPIC's data protection officer has the following tasks in particular: responding to requests for information, examining the processing of personal data by the FDPIC office and recommending corrective action if a breach

of data protection regulations is identified. The data protection officer also oversees the review, enforcement and updating of data processing regulations.

The FDPIC's IT security officer is the point of contact for the IT security officer of the Federal Chancellery, whereby the Federal Chancellery is responsible for the IT security of all infrastructures and applications that it operates for the FDPIC. Within our organisation, the IT security officer is the central point of contact for data security issues. The IT security officer also monitors the development and implementation of the Federal Chancellery's data security requirements in relation to the FDPIC and participates in awareness-raising activities.

3.2 Communication

New website with reporting portals

During the year under review, the FDPIC's communications team continued work on the new website to bring its content into line with the revised Federal Act on Data Protection. The new website was successfully launched on 11 May 2023 and has been continually updated since then. In particular, the team have compiled and uploaded a wealth of information and resources on the new legal provisions. The three new reporting portals and the various contact forms are being actively used and make it easier for data subjects and data controllers to get in touch with the FDPIC (see also Focus I).

Figures

The FDPIC released information to the public about twice a month, issuing six press releases and 20 'news in brief' items concerning recently launched or concluded procedures (clarification of

the facts under the old law or investigations under the new law) or important current data protection issues or events that were the subject of public debate. In addition to the 45 recommendations published in 2023, the FDPIC also commented on the Freedom of Information Act: The use of emergency legislation to restrict the Freedom of Information Act in connection with the Credit Suisse case reminds us of the emergency decisions taken during the Covid pandemic and raises fundamental legal questions.

The Federal Administration's digitalisation projects came under increased public scrutiny, be it the as yet unsuccessful attempt to recover vaccination data from the *meineimpfungen.ch* platform (see Section 1.4) and the plan to include vaccination data in the

electronic patient dossier (EPD), the creation of a state-recognised electronic identity (e-ID), or the Federal Cloud Strategy with the introduction of Microsoft 365 and the switch to the public cloud of a large US company. The FDPIC oversees the Confederation's large-scale digital projects in a supervisory capacity to ensure that they are implemented in compliance with data protection regulations (see Section 1.1).

Issues

Cyber security remains a hot topic in public debate. The media report on unauthorised access to data on a daily basis, and the FDPIC is often asked to comment on cyber incidents in Switzerland. In the case of the hacker attack on the company Xplain, the FDPIC launched an investigation into the Federal Office of Police (fedpol) and the Federal Office for Customs and Border Security (FOCBS) after receiving reports of potentially serious breaches of data protection regulations. Shortly afterwards, the investigation was extended to the company in question (see Section 1.2).

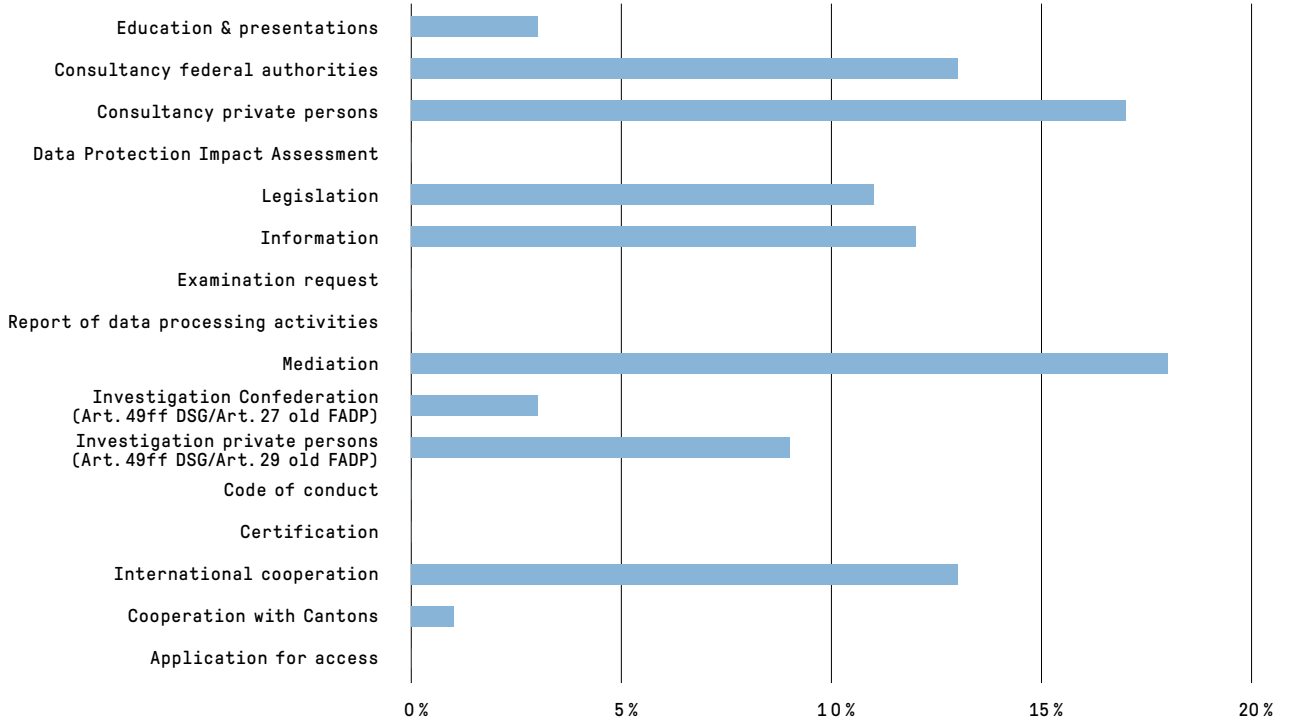
During the year under review, the FDPIC also received numerous enquiries about the increasingly popular phenomenon of artificial intelligence (AI). The increasing use of AI-based applications is causing public concern, and media monitoring shows that fears of constant surveillance are on the rise, be it in public spaces at railway stations, while shopping in supermarkets or even in the bedroom, for example with health apps that record rest periods. At the same time, AI applications are increasing the risk of disinformation, with fake news being used to manipulate users of online services and making it harder for the public to form an opinion. Identity theft is also an increasing concern.



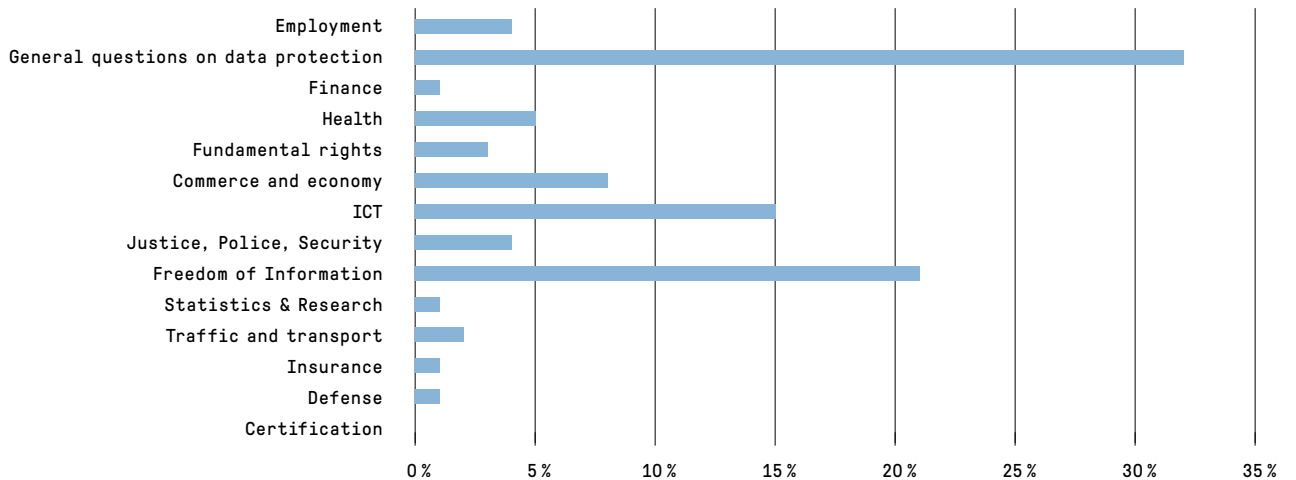
3.3 Statistics

Statistics on FDPIC's activities from 1st April 2023 to 31 March 2024 (Data protection)

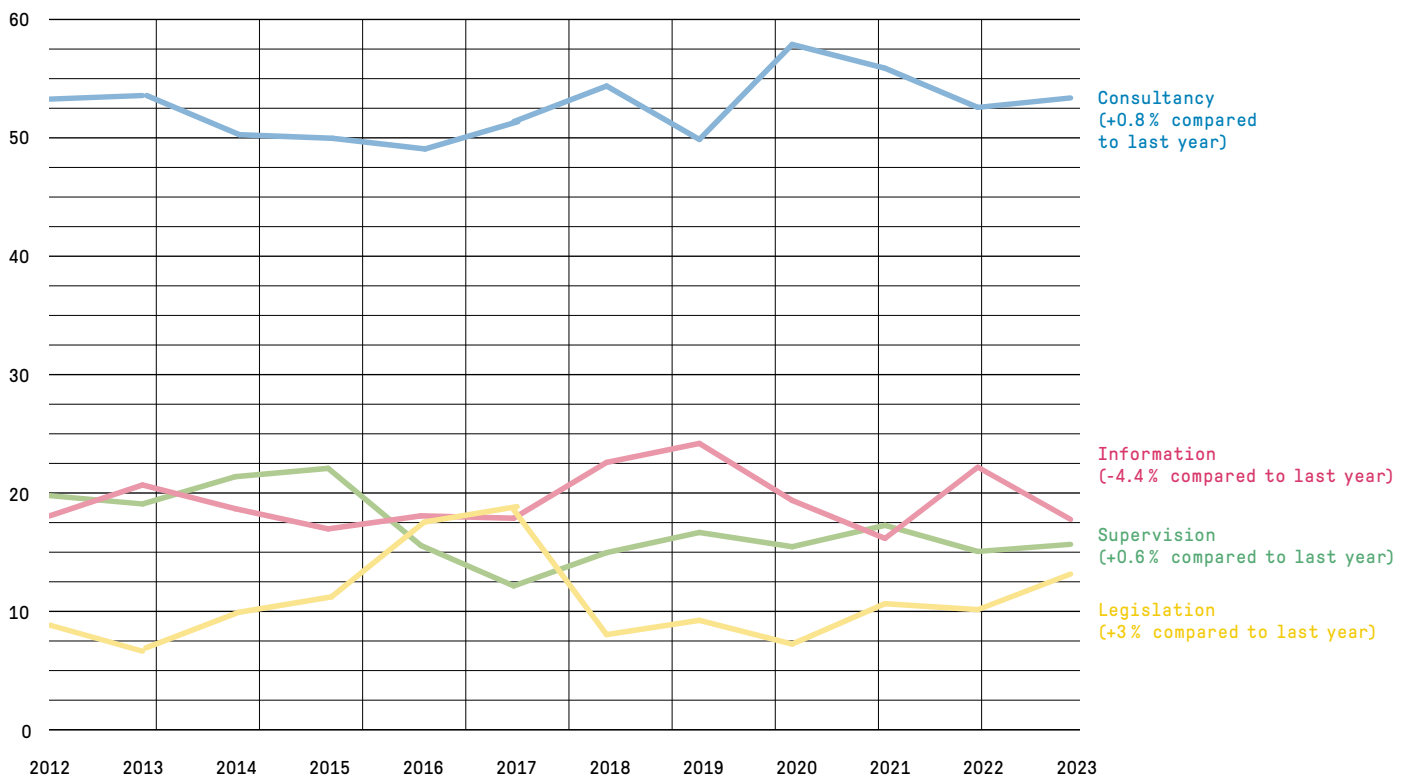
Workload per tasks



Workload per material



Multi-year comparison
(as a percentage)



Overview of applications for access under the Freedom of Information Act from 1st January to 31 December 2023

Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
BK	90	43	21	18	0	5	3
EDA	228	87	23	62	5	18	33
EDI	230	81	16	67	25	26	15
EJPD	152	80	14	27	9	5	17
VBS	432	309	9	72	6	9	27
EFD	191	52	41	63	9	14	12
WBF	175	80	27	39	5	6	18
UVEK	236	97	24	54	14	13	34
BA	2	1	0	0	0	0	1
PD	2	0	1	0	0	0	1
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)	-
Total 2013 (%)	470 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	-

Statistics on applications for access under the Freedom of Information Act from 1st January to 31 December 2023

		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 Chancellery FCh	FCh	76	0	33	20	18	0	2	3
	FDPIC	14	0	10	1	0	0	3	0
	Total	90	0	43	21	18	0	5	3
Federal Department of Foreign Affairs FDFA	FDFA	228	0	87	23	62	5	18	33
	Total	228	0	87	23	62	5	18	33
Federal Department of Home Affairs FDHA	GS FDHA	19	0	5	4	3	5	0	2
	FOGE	3	0	2	0	0	0	1	0
	FOC	7	2	6	0	1	0	0	0
	SFA	1	1	1	0	0	0	0	0
	METEO CH	0	0	0	0	0	0	0	0
	NL	0	0	0	0	0	0	0	0
	FOPH	76	4	21	3	28	8	15	1
	FOS	10	0	7	1	0	0	1	1
	FSIO	10	0	9	0	0	0	0	1
	FSVO	33	0	13	3	10	3	1	3
	SNM	0	0	0	0	0	0	0	0
	SWISS MEDIC	67	3	13	5	25	9	8	7
	SUVA	4	0	4	0	0	0	0	0
	compenswiss	0	0	0	0	0	0	0	0
Total	230	10	81	16	67	25	26	15	
Federal Department of Justice and Police FDJP	GS F DJP	15	0	9	0	2	0	2	2
	FOJ	34	0	20	5	2	0	0	7
	FEDPOL	13	0	2	6	2	1	0	2
	METAS	3	0	2	1	0	0	0	0
	SEM	70	0	36	0	20	8	3	3
	PTSS	3	0	0	0	1	0	0	2
	SIR	8	0	5	2	0	0	0	1
	IPI	4	0	4	0	0	0	0	0
	FGB	2	0	2	0	0	0	0	0
	ESchK	0	0	0	0	0	0	0	0
	FAOA	0	0	0	0	0	0	0	0
	ISC	0	0	0	0	0	0	0	0
	NKVF	0	0	0	0	0	0	0	0
	Total	152	0	80	14	27	9	5	17

		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 Defence, Civil Protection and Sport DDPS	GS DDPS	83	2	17	5	41	4	5	11
	Defence	17	0	3	1	2	1	2	8
	FIS	31	0	3	2	19	0	1	6
	OA-IA	1	0	0	1	0	0	0	0
	armasuisse	8	0	2	0	4	0	1	1
	FOSPO	277	0	276	0	0	1	0	0
	FOCP	8	0	5	0	3	0	0	0
	swisstopo	7	0	3	0	3	0	0	1
	OA	0	0	0	0	0	0	0	0
	Total	432	2	309	9	72	6	9	27
Federal Department of Finance FDF	GS FDF	87	0	18	24	31	4	3	7
	FFA	10	0	4	1	3	1	0	1
	FOPER	3	0	2	0	0	0	0	1
	FTA	24	0	10	5	6	2	0	1
	FCA	31	7	3	7	14	0	6	1
	FOBL	7	3	7	0	0	0	0	0
	FOITT	6	0	0	0	5	1	0	0
	SFAO	6	0	3	1	2	0	0	0
	SIF	14	0	3	2	2	1	5	1
	PUBLICA	1	0	0	1	0	0	0	0
	CCO	2	0	2	0	0	0	0	0
	Total	191	10	52	41	63	9	14	12

		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	11	0	1	3	4	0	0	3
	SECO	47	2	7	13	20	0	2	5
	SERI	7	0	3	0	1	1	0	2
	FOAG	16	0	11	0	2	0	2	1
	Agroscope	0	0	0	0	0	0	0	0
	FONES	7	2	2	1	2	1	0	1
	FHO	3	0	2	0	1	0	0	0
	PUE	10	0	2	2	6	0	0	0
	COMCO	18	1	9	6	1	2	0	0
	ZIVI	0	0	0	0	0	0	0	0
	FCAB	1	0	1	0	0	0	0	0
	SNSF	1	0	0	0	0	0	1	0
	SFIVET	0	0	0	0	0	0	0	0
	ETH Board	53	0	42	2	1	1	1	6
	Innosuisse	1	0	0	0	1	0	0	0
	Total	175	5	80	27	39	5	6	18

Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	24	0	10	1	0	0	1	12
	FOT	9	0	5	0	2	0	1	1
	FOCA	27	5	7	8	7	2	1	2
	SFOE	20	0	2	1	10	1	1	5
	FEDRO	17	0	15	0	1	0	0	1
	OFCOM	24	0	9	0	4	4	2	5
	FOEN	98	1	44	11	26	7	4	6
	ARE	3	0	3	0	0	0	0	0
	ComCom	1	0	0	0	0	0	0	1
	ENSI	6	2	0	0	2	0	3	1
	ESTI	1	0	0	0	1	0	0	0
	PostCom	3	2	2	0	1	0	0	0
	ICA	1	0	0	1	0	0	0	0
	FPI	0	0	0	0	0	0	0	0
	SUST	2	0	0	2	0	0	0	0
	Total	236	10	97	24	54	14	13	34

		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
Office of the Attorney General OAG	OAG	2	0	1	0	0	0	1
	Total	2	0	1	0	0	0	1
Parliamentary Services PS	PS	2	0	0	1	0	0	1
	Total	2	0	0	1	0	0	1
Total sum		1738	37	830	176	402	73	161

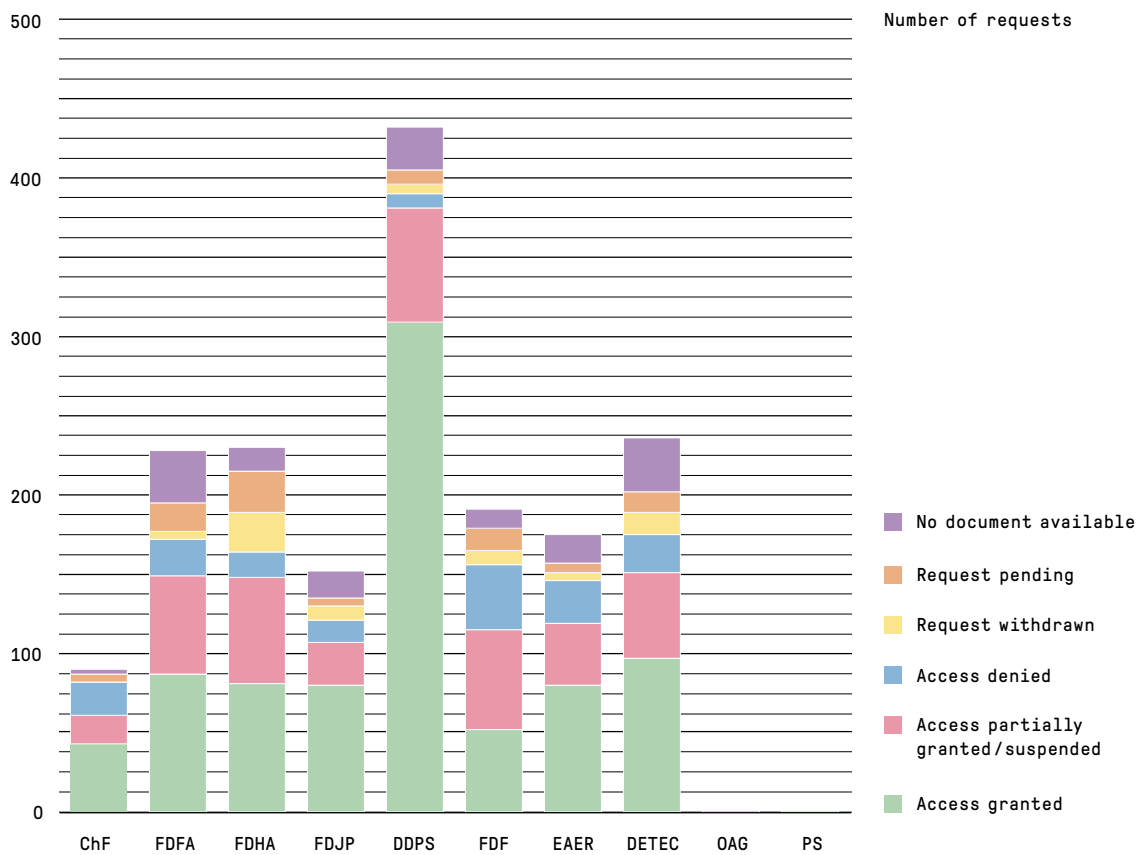
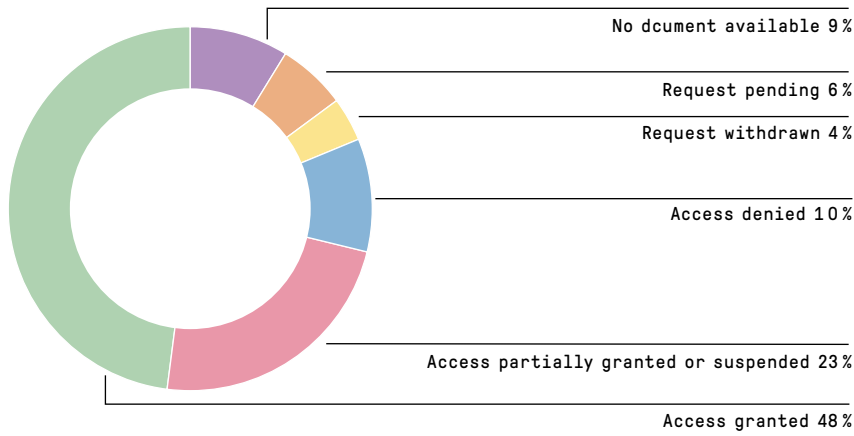
Requests for access 2023 with Corona reference

		Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/ suspended	Request withdrawn	Pending requests	No document available
Federal Chancellery FCh	Total	0	0	0	0	0	0	0
Federal Department of Foreign Affairs FDFA	Total	0	0	0	0	0	0	0
Federal Department of Home Affairs FDHA	FOPH	22	9	0	11	0	2	0
	FOS	1	0	0	0	0	0	1
	swissmedic	12	2	1	5	0	0	4
	Total	35	11	1	16	0	2	5
Federal Department of Finance FDF	Total	0	0	0	0	0	0	0
Federal Department of Justice and Police FDJP	Total	0	0	0	0	0	0	0
Federal Department of the Environment, Transport, Energy and Communications DETEC	OFCOM	1	0	0	1	0	0	0
	ComCom	1	0	0	0	0	0	1
	Total	2	0	0	1	0	0	1
Federal Department of Defence, Civil Protection and Sport DDPS	Total	0	0	0	0	0	0	0
Federal Department of Economic Affairs, Education and Research EAER	SECO	1	0	0	0	0	0	1
	ETH Board	1	1	0	0	0	0	0
	Total	2	1	0	0	0	0	1
Office of the Attorney General	OAG	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0
Parliamentary Services	PD	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0
	Total sum	39	12	1	17	0	2	7

Number of requests for mediation by applicant category

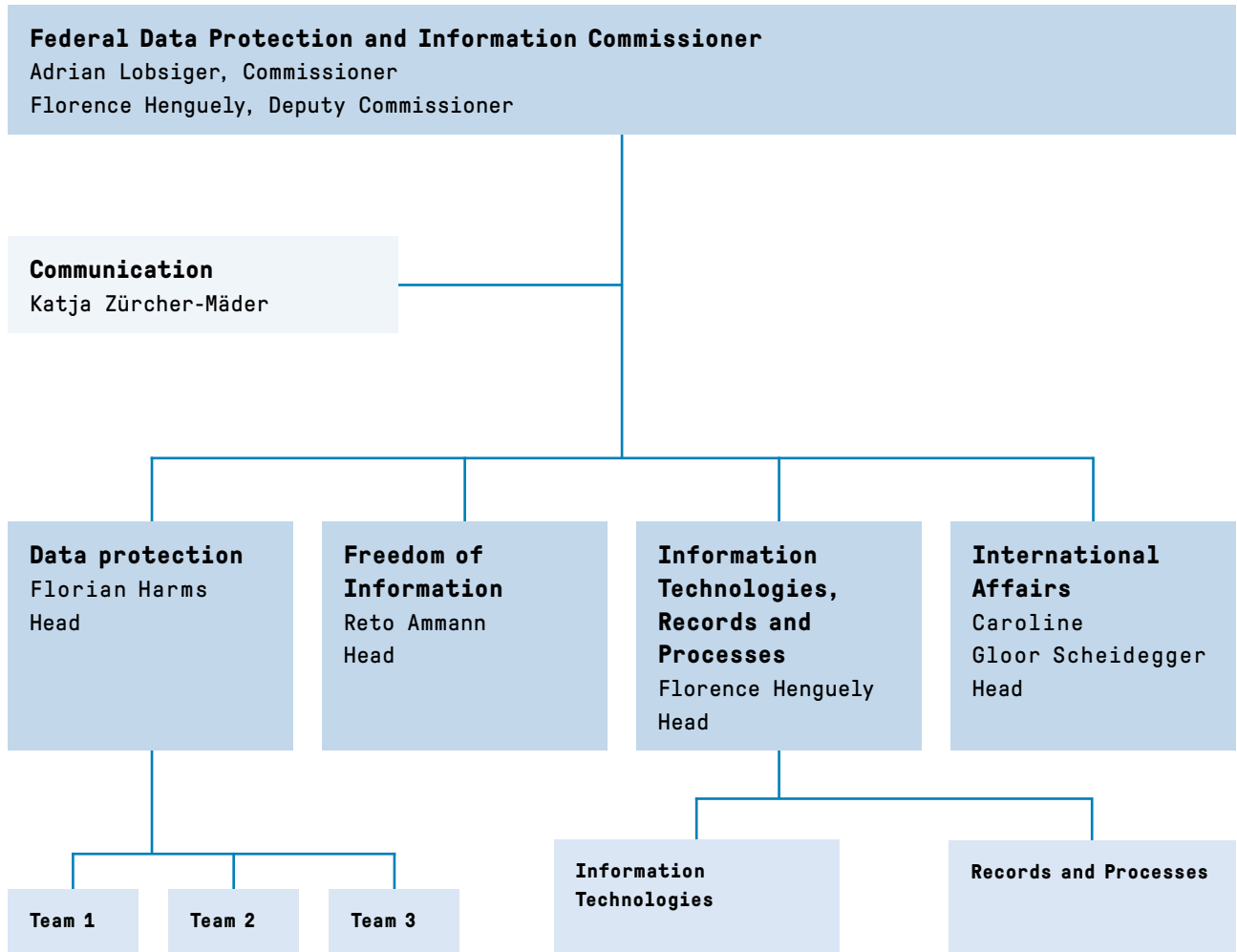
Applicant category	2023	2022	2021	2020	2019	2018	2017
Media	74	47	53	31	34	24	21
Private individuals (or no exact assignment possible)	31	37	49	42	40	26	35
Stakeholders (associations, organisations, clubs etc.)	8	9	16	5	7	9	14
Lawyers (for third parties or on their own account)	16	27	12	7	5	4	2
Companies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

**Applications for access in the federal administration
from 1st January to 31 December 2023**



3.4 Organisation FDPIC (Status 31 March 2024)

Organisation chart



Employees of the FDPIC

Number of employees	47		
FTE	40.2		
per gender	Women	24	51%
	Men	23	49%
by employment level	1-89%	28	60%
	90-100%	19	40%
by language	German	35	75%
	French	11	23%
	Italian	1	2%
by age	20-49 years	27	57%
	50-65 years	20	43%
Management	Women	6	55%
	Men	5	45%

Abbreviations

AI Artificial intelligence

ArchA Archiving Act

DPCO Ordinance on Data Protection Certification

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

DPO Ordinance to the Federal Act on Data Protection

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

FADP Federal Act on Data Protection

FDPIC Federal Data Protection and Information Commissioner

Fedpol Federal Office of Police

FoIA Freedom of Information Act

FoIO Ordinance on Freedom of Information in the Administration

GDPR General Data Protection Regulation

GPA Global Privacy Assembly

HRA Human Research Act

ICT Information and Communication Technology

ITSOO Information and Communication Technology

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

Figure 1: Evaluation of requests for access – trend since 2010 p. 65

Figure 2: Fees charged since the FoIA entered into force.....p. 67

Figure 3: Mediation requests since the FoIA entered into force..... p. 68

Tables

Table 1: Amicable outcomes p. 69

Table 2: Processing time of mediation procedures p. 70

Table 3: Pending mediation procedures p. 71

Table 4: Special provisions under Art. 4 FoIA p. 78

Table 5: No special provisions under Art. 4 FoIA p. 79

Table 6: Staff positions available for FADP issues..... p. 82

Table 7: Services in data protection.... p. 82

Table 8: Consultancy for large-scale projects in 2023 p. 83

Table 9: Outcome objectives for FDPIC p. 84

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. 410.031.ENG

Layout: Ast & Fischer AG, Wabern

Photography: Monika Flückiger

Characters: Pressura, Documenta

Print: Ast & Fischer AG, Wabern

Paper: PlanoArt[®], woodfree bright white



Key figures

Workload data protection

53%

Consultancy

16%

Supervision

18%

Information

13%

Legislation

Applications for access Freedom of Information (FoIA)

48%

granted

23%

partially granted
or suspended

10%

denied

4%

withdrawn

6%

pending

9%

no document
available

Data protection concerns



Fair information

Companies and federal bodies provide transparent information on their data processing: comprehensible and complete.



Freedom of Choice

Those affected from data processing (data subjects) give their consent on the basis of transparent information and are provided with genuine freedom of choice.



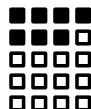
Risk analysis

The possible data protection risks are already identified in the project and their effects minimized with measures.



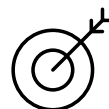
Data correctness

The processing takes place with applicable data.



Proportionality

No data collection on stock, but only as far as necessary to achieve the purpose. Data processing is limited in scope and time.



Purpose

The data will be processed only for the purpose indicated at the time of collection, as indicated by the circumstances or as provided for by law.



Data security

The data processor ensures adequate security of personal data – both at the technical and organizational level.



Documentation

All data processing is documented and classified by the data processor.



Responsibility


Private and federal bodies are responsible for fulfilling their obligation to comply with data protection legislation.

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

E-Mail: info@edoeb.admin.ch

Website: www.thecommissioner.ch

 @EDÖB – PFPDT – IFPDT

 @derBeauftragte

Phone: +41 (0)58 462 43 95 (Mo–Fr, 10 am – 11:30 pm)

Fax: +41 (0)58 465 99 96