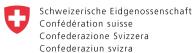


30th **Annual Report 2022/23** Federal Data Protection and Information Commissioner



Annual Report 2022/2023

Federal Data Protection and Information Commissioner

The Commissioner shall submit a report to the Federal Assembly at regular intervals and as required. He shall provide the Federal Council with a copy of the report at the same time (Art. 30 FAPD).

This report covers the period between 1 April 2022 and 31 March 2023 for the section on data protection. For the section on freedom of information it corresponds to the calendar year 1 January to 31 December 2022.



Foreword

The first Federal Act on Data Protection of 19 June 1992 came into force on 1 July 1993. In its legislative dispatch of 23 March 1988, the Federal Council had already justified the need for legislative action based on the use of modern information and communication technologies in virtually all areas of life and the rapid intensification of data processing and its spread throughout society, the economy and government.

Thirty years on, almost every aspect of our lives is digital, which no one could have predicted back then. With today's digital society permanently connected to the internet via smartphone as it goes about its daily business, from banking to online dating, the scope and intensity of personal data processing has grown exponentially.

The fully revised Federal Act on Data Protection of 25 September 2020 is scheduled to come into force on 1 September 2023. This new act provides businesses, the Federal Administration and the federal data protection supervisory authority with new modern instruments to meet the public's legitimate expectations in terms of robust protection of privacy and informational self-determination in accordance with the rule of law.

The work of the FDPIC team in preparation for the transition to the new law is in full swing and is proceeding according to plan (see Focus).

Adrian Lobsiger

Federal Data Protection and Information Commissioner

-1. Myn

Bern, 31 March 2023

- Dating-Apps: Analysis of the data processing

organiser

- Virtual races: Improved data protection at a virtual race

Current Challenges	6 1.4 Health			
Data protection	 National organ donor register NODR: Insufficient online authentication 			
1.1 Digitalisation and fundamental rights	- Online registers: Data protection risks in the breast implant register			
 Federal cloud strategy: Challenging cloud project of Federal Chancellery 	the – Lack of security: Investigation into database of private Covid-19 test centers			
 National data management: SpiGes project of the FSG Certification: New Ordinance on Data Protection 	 Online platform: Project to recover vaccination data of meineimpfungen.ch platform 			
Certification (DPCO)	- Electronic patient records: New developments			
 Votes and elections: Updating of the existing guideling Electronic identity (E-ID): Self-sovereign identity 	nes – Electronic invoicing: Legal obligation to send copies of medical invoices			
approach - Swiss Post's online portal: Access with Swiss ID only	- Electronic invoicing: Project regarding the transmission of electronic invoices in compulsory health insurance			
now on	1.5 Employment			
 Digital Switzerland strategy: Digital driving licence project 	- Federal employees: Retention of staff records by the FSO			
Focus	1.6 Traffic and transport			
30 years of data protection in Switzerland	 Swiss Federal Railways: Passenger flow measurement at railway stations 			
1.2 Justice, Police, Security	26 1.7 International 50			
- FOCBS: Customs Act	 Europe: Council of Europe 			
- Protection status S: Web application RegisterMe	 Europe: European Data Protection Commissioners' Conference in Dubrovnik 			
 Mitto AG: Preliminary clarification on possible misuse the 'signalling system access' 	е от – Europe: European Case Handling Workshop			
the digitaling system assess	 International: Global Privacy Assembly 			
1.3 Commerce and economy	30 – Humanitarian aid: GPA working group			
 Disclosure of personal data to foreign tax authorities The Federal Supreme Court rules against the right to 	Authorities			
information of third parties in international administr assistance in tax matters	rative – Bilateral: Visit by a Tunisian delegation			
Tracking technologies: Investigation into a possible bre	- International cooperation: Privacy Symposium in Venice			
of Swiss people's right to privacy by Oracle	- Schengen: BTLE and EDPB			
- Postfinance: Waiving account publicity	- Schengen: Supervision Coordination Groups on the SIS II,			
- Credit-history checks: Database entries based on po	or VIS and Eurodac information systems			
household credit history	- Schengen: Schengen Coordination Group of the Swiss data protection authorities			
 Cyberattack: Preliminary investigation into Infopro A Fiducial Winbiz SA 	 Schengen: Schengen-related activities at the national 			
 Preliminary investigation at a voice service provider: Security vulnerability promptly fixed 	level			

2.1 **General** 62 3.1 Duties and resources85 Services and resources in the field of data protection 2.2 Applications for access slightly - Services and resources in the field of freedom of down in 2022......64 information - Participation in committee consultations and 2.3 Mediation procedures: parliamentary committee hearings mediation requests slightly down..........68 - Proportion of amicable outcomes 3.2 Communication 88 - Duration of mediation procedures - Figures - Number of pending cases - Main focus areas Data sharing and trading 2.4 Legislative process72 - New website - Cybersecurity: The amendment of the Information Security Act (ISA) 3.3 Statistics 90 - Electricity industry: Preliminary draft of the Federal Act - Statistics on FDPIC's activities from 1st April 2022 on a "rescue umbrella" for the electricity industry to 31 March 2023 (Data protection) - Archiving Act: Revision of the Federal Act on Archiving - Overview of applications from 1st January to 31 December 2022 - Finance: Entry into force of the Anti-Money Laundering - Statistics on applications for access under the Freedom Act and Anti-Money Laundering Ordinance of Information Act from 1st January to 31 December 2022

The FDPIC

- Requests for access 2022 with Corona reference

from 1st January to 31 December 2022

Organisation chartEmployees of the FDPIC

In the cover - Key figures

- Data protection concerns

Number of requests for mediation by applicant category

- Applications for access in the federal administration

3.4 Organisation FDPIC......100

Figures and tables 103

Freedom of Information

- Tobacco control Act: Partial revision of the Federal Act on

Art. 4 FoIA80

- Economy: New Federal Act on the Screening of Foreign

Tobacco Products and Electronic Cigarette

Investments (IPG in German)

2.5 Special reservations under

Current Challenges

I Digitalisation

Digital responsibility

Digital transformation is a phenomenon that affects society as a whole and raises important issues concerning the authorities, businesses, users and the general public. Instead of blindly submitting to technological advances, we need to analyse the processes at play in order to ensure that digital technology is used responsibly in the service of the people.

Digital responsibility plays a key role in this context – a broad concept including financial, legal, ecological, social and ethical considerations. While digitalisation offers considerable potential, it also poses new risks for data controllers. Therefore, the FDPIC believes that digital responsibility is now an integral part of good governance. Digital responsibility includes compliance with legislation, which protects privacy rights when personal data is processed.

The revised Federal Act on Data Protection (FADP, see Focus) requires data controllers to take a proactive approach to automated processing and digitalisation. It provides controllers with tools for performing general and specific analyses of data processing operations and methods as well as techniques for creating transparency, trust and credibility vis-à-vis data subjects. Although zero risk is virtually unattainable in the processing of personal data, the tools provided enable data controllers to identify, mitigate and responsibly manage residual risks and thus protect the privacy and informational self-determination of all data subjects.

A proactive approach is also crucial for technical security, especially when it comes to preventing cyber-attacks. The Meineimpfungen and Swisstransplant scandals featured in Section 1.4 show just how important the rules and tools of the new Act are for safeguarding fundamental rights and promoting digital responsibility.

Supervisory support and risk-based project management

The practical meaning of 'digital responsibility' in the sense of business practice accountability becomes apparent in the consultancy services that the FDPIC provides to digital project managers in the business sector in his role as a supervisory authority: Under Swiss data protection law, private individuals are in principle allowed to process personal data without official authorisation.

"As the data protection supervisory authority, the FDPIC does not issue authorisations."

Therefore, as the data protection supervisory authority, the FDPIC does not issue authorisations. In his consultations, he works to ensure compliance with the requirements of data protection legislation. That said, all responsibility for the projects implemented ultimately rests with the project owners. The FDPIC also makes project owners aware of aspects of their digital responsibility that may go beyond the requirements of data protection legislation: For example, the psychological repercussions of data collection methods employed by private individuals in work settings, stores or commercial meeting

places. Data collection can create a 'chilling effect', whereby people will alter their behaviour in contexts in which data is collected, which effectively restricts their self-determination. This chilling effect can be caused not only by the intensity of data collection but also by the widening or blurring of purposes for which data is processed. The degree of restraint that project managers should exercise, taking into account the chilling effect, when collecting data within the limits tolerated by data protection legislation is essentially a matter of business strategy and digital responsibility (see Section 1.6 Traffic and transport).

However, the legislator of the new FADP also imposes restrictions on digital responsibility, which the Commissioner will enforce by strengthening his supervisory activity. If project managers become aware during the

planning stage that the data processing operations they are planning are likely to result in high risks, the new FADP requires them to carry out a data protection impact assessment (DPIA) in good time in order to assess the potential risks in more detail and to take appropriate protective measures to reduce them. If the findings of the DPIA suggest that the potential risks remain high even with appropriate protective measures in place, the new FADP still does not prohibit the processing operations from going ahead all the same. However, in this case the Act requires that data controllers contact the FDPIC in advance and submit their DPIA to him.

"The 'chilling effect' can lead to people being restricted in their self-determined way of life." The FDPIC will then check whether the DPIA submitted to him presents the identified risks in a clear, comprehensible and complete manner and whether the planned data processing operations, taking into account the risks, are compatible with data protection legislation as a whole in the sense that they are deemed reasonable as far as the data subjects are concerned in terms of the envisaged scope and intensity and are therefore generally considered acceptable. The FDPIC will submit any objections and recommendations

for improvement regarding the content of the DPIA or the planned processing operations themselves to the data controller within two months. Objections may be raised with regard to the content of the DPIA, for example, when the controller is reluctant to adequately assess and transparently disclose potential risks. The FDPIC's opinion does not constitute approval of a planned project.

If a data controller refuses to take on board important objections and recommendations, the FDPIC may take supervisory action, open an investigation and formally order the recommended changes or additions or even go as far as prohibiting the processing operations altogether in due course. The FDPIC may take formal action if

data subjects cannot be expected to accept a risk, particularly in cases where there is a high risk of serious privacy violations, and therefore the planned processing operations are deemed inadmissible under data protection law – for example, where data processing operations presenting a high residual risk would violate data protection principles under Art. 6 nFADP (e.g. proportionality) or technical security requirements under Art. 8 nFADP.

"The legislator of the new FADP imposes restrictions on digital self-responsibility, which the Commissioner will enforce by strengthening his supervisory activity."

II Growing number of exceptions to the Freedom of Information Act in specific legislation and emergency legislation

In the Emergency Ordinance of 16 March 2023 on Additional Liquidity Assistance Loans and the Granting of Federal Default Guarantees for Liquidity Assistance Loans made by the Swiss National Bank to Systemically Important Banks, the Federal Council stipulated, inter alia, that no access to official documents will be granted under the Freedom of Information Act. The exclusion of citizens' rights of access guaranteed by the Freedom of Information Act by way of an emergency ordinance raises fundamental legal issues.

Following the pandemic, during which many decisions were made under emergency legislation, and the "rescue umbrella" for the electricity sector, with the aforementioned ordinance of 16 March 2023 the Federal Council has once again, within a short period of time, decreed that activities which it has delegated to the Administration by means of emergency legislation will not be subject to the Freedom of Information Act, using that

same emergency legislation. Both cases may entail the use of billions of francs of taxpayers' money.

The Federal Council's approach raises fundamental legal issues: based on the information currently available to the FDPIC, in neither of these cases does the justification provided for enacting emergency legislation based directly on the Federal Constitution in order to support the electricity or financial sectors explain the necessity to exclude by emergency legislation the citizens' right to information about the activities of the Administration based on that emergency legislation. If there is no need to restrict citizens'

rights under the Freedom of Information Act by emergency legislation, the question arises as to where the Federal Council derives the right to repeal this federal act by ordinance.

Had the Freedom of Information Act continued to apply, the Federal Administration would have been able in both cases to restrict access to official documents under this Act, citing the protection of public and private interests, or at least to defer such access until the Federal Assembly may decide to exclude administrative transparency through the ordinary legislative procedure, and – if it deemed such exclusion necessary – to anchor it in a formal enactment.

In view of the accelerating growth in the number of special legal exclusions of the FoIA, the Commissioner has decided to publish a table starting with this annual report, which will henceforth show the current status of these exclusions (s. ch. 2.5).

9

"The exclusion of citizens' rights of access guaranteed by the Freedom of Information Act by way of an emergency ordinance raises fundamental legal issues."

III National and international cooperation

Strengthening cooperation with the cantons

In the ongoing digital transformation, the processing of personal data is becoming increasingly complex, involving a large number of public and private players and increasing the cascade of data processing by third parties. This phenomenon comes to the fore whenever cyber attacks and data security breaches are reported, such as in the cases of Infopro and Winbiz (see Section 1.3).

Cooperation is being intensified in order to ensure effective and comprehensive monitoring, particularly in relation to federal and cantonal data protection legislation. This applies in particular in cases where cantonal or communal public authorities employ private individuals to process data, or where private or public entities also act under private law or are vested with public authority, or where there are cantonal regulations under which the Federal Act on Data Protection applies.

The FDPIC has made this one of the points of his strategy for 2023, namely the strengthening of cooperation with his cantonal and communal counterparts on transparency and data protec-

tion in order to travel the digital transformation road together while respecting their remits and independence.

In preparation for the 2023 federal elections, the FDPIC and the bureau of the Conference of Swiss Data Protection Commissioners (privatim) have updated their guide to the digital processing of personal data in connection with elections and votes in Switzerland (see Section 1.1).

In addition, the data protection authorities will continue to work on the issue of cloud computing, particularly with regard to the transfer of databases, applications and on-premise IT processes to the cloud. In this regard, the FDPIC is closely monitoring developments in the European Union and is also in contact with the parties concerned.

"The federal, cantonal and communal data protection authorities aim to strengthen their cooperation."

Council of Europe

The Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) is also open to accession by non-member states of the Council of Europe. Russia's extraordinary withdrawal from the Council of Europe has forced the Consultative Committee to consider the conditions of continued participation in such cases (see Section 1.7). Active participation in the Committee is particularly important for the modernised Convention 108 (Convention 108+). This Convention is considered an important tool and constitutes a bridge between different regions of the world and between different national legislative frameworks. The FDPIC continues to participate actively in the Committee.

International cooperation

The disclosure of personal data to a country without an adequate level of data protection raises similar privacy questions in different countries. The FDPIC is specifically monitoring developments in this area in EU and EEA Member States, particularly in connection with the ongoing talks between the EU and the US on this issue.

Evaluation of the level of data protection

Switzerland is still waiting for the EU to recognise Swiss data protection law as offering an adequate level of protection in accordance with the GDPR. which came into force in 2018. In the meantime, its adequacy decision of 2000 remains in force. This decision was made based on the former Data Protection Directive 95/46/EC, which was later replaced by the GDPR. The EU Commission is expected to publish its adequacy reports on all the states that were already considered adequate pre-GDPR at the same time, namely Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand and Uruguay. It is hoped that the EU Commission will issue its new adequacy decision regarding Switzerland in 2023.

"It is to be hoped that the EU Commission will make its new adequacy decision for Switzerland in the course of the year 2023."

Data protection

1.1 Digitalisation and fundamental rights

FEDERAL CLOUD STRATEGY

Challenging cloud project of the Federal Chancellery

During the year under review, the FDPIC dealt with issues relating to the implementation of the Federal Administration's cloud strategy. He participated in a number of office consultations and advised the Federal Chancellery on its Cloud Enabling Office Automation (CEBA) project.

During an office consultation, the Federal Chancellery's Digital Transformation and ICT Steering (DTI) sector presented the cloud principles that are part of the Federal Administration's cloud strategy to the FDPIC. These serve as recommendations for the procurement of cloud applications by the various administrative units.

The FDPIC demanded, among other things, that the DTI's recommendations constitute binding minimum requirements, which the departments may choose to make more stringent but never more relaxed. Furthermore, the FDPIC found that the principles were strongly influenced by the information security perspective and thus

did not take due account of data protection issues. In particular, the principles drew on a distinction between sensitive personal data and other personal data, which, in the FDPIC's view, was not a very suitable criterion for assessing the risks to the privacy and fundamental rights of data subjects, especially since combining non-sensitive personal data could also result in a high processing risk. A high risk can result from the use of new technologies or the nature, scope, context or purposes of the processing, all elements that are typically encountered in cloud outsourcing. Therefore, the FDPIC insisted that the cloud principles should require a data protection impact assessment when personal data was to be processed in the cloud.

The DTI sector involved the FDPIC in its preliminary work on the intro-



duction of Microsoft 365, in particular by submitting to him the drafts of an analysis of the legal requirements and the in-

formation security and data protection (ISDP) concept. In his comments, the FDPIC stated, among other things, that in his view it was uncertain how long it would remain technically feasible to run certain applications at the federal government's own IT centers rather than in the cloud operated by the US company Microsoft, as the DTI project

envisages today. In view of this uncertainty, the FDPIC requested that alternatives to Microsoft 365 be put forward that are less problematic from a data protection perspective. He went on to request a more detailed analysis as to whether a sufficient legal basis existed for the processing of personal data in the cloud operated by Microsoft, and whether the principle of proportionality was observed. Regarding the distinction between sensitive personal data and other data by users themselves, in the FDPIC's view it remains unclear whether this is appropriate or feasible. Finally, he urges the DTI to carry out a comprehensive data protection impact assessment transparently highlighting the risks of outsourcing to the cloud. In his opinion, a detailed analysis is crucial to assess the issue of possible access by the US security authorities to personal data that the Federal Administration processes in the Microsoft cloud.

SpiGes project of the FSO

During the year under review, the Federal Statistical Office submitted a report to the FDPIC on the status of the project regarding the reuse of data from inpatient hospital stays (SpiGes). The FDPIC pointed out the privacy risks inherent to this sub-project of the National Data Management (NaDB) programme and demanded that appropriate protective measures be developed for its implementation.

The National Data Management (NaDB) programme was launched in October 2019 under the lead of the FSO and aims to allow the reuse of data and to facilitate data sharing between authorities. One of the pilot projects of the NaDB programme is the reuse of data collected within the context of inpatient hospital healthcare (SpiGes project). The project involves collecting data from inpatient hospital stays once only via the FSO's interoperability platform in accordance with the once-only principle and then using the data for both administrative and statistical purposes (see also 29th Annual Report, Section 1.1).

One specific risk that can arise when data is reused and which the FDPIC



has explicitly highlighted is the violation of the 'limitation of purpose' principle. To prevent this, a clear distinction must be

made between data processing for statistical purposes and data processing for other (e.g. administrative) purposes. Furthermore, special attention needs to be given to operators with the dual role of data providers and data recipients, such as hospitals and insurance companies. A clear IT and organisational separation of the data categories processed and restricted access to these separate data categories are therefore essential.

In this regard, the FDPIC pointed out to the FSO that, given the scope of the project and the high risk associated with the extensive processing of sensitive personal data, risk analyses needed to be carried out to assess the privacy risks and determine the action needed to address such risks, in accordance with the new Federal Act on Data Protection in particular, which is due to come into force in September 2023 (Article 22 nFADP, Data Protection Impact Assessment).

CERTIFICATION

New Ordinance on Data Protection Certification (DPCO)

In the year under review, the FDPIC

advised the Federal Office of Justice in its legislative work on the new Ordinance on Data Protection Certification (DPCO). The Federal Council has issued the Ordinance on Data Protection Certification (DPCO) of 31 August 2022 regulating the recognition of certification procedures and the introduction of a data protection quality label. The ordinance is due to come into force with

the new FADP on 1 September 2023.

The FDPIC worked with the Swiss Accreditation Service (SAS) to support the Federal Office of Justice in fleshing out the DPCO, advising it on legal and IT aspects. In addition, the FDPIC is currently developing specific guidelines regarding the minimum requirements for a management system as well as guidelines for the data protection criteria to be applied when assessing the conformity of products, services and processes.

When data is processed in connection with certified systems, products or services, data controllers are not required to carry out a data protection



VOTES AND ELECTIONS

Updating of the existing guidelines

Self-sovereign identity

ELECTRONIC IDENTITY (E-ID)

impact assessment, even where there is a high risk to personal privacy. Certification also enables manufacturers and data controllers to document their



compliance with the Data Protection Act. In the FDPIC's view, data protection certification can strengthen data protec-

tion in Switzerland. In particular, certification promotes transparency by having increasingly complex data processing operations analysed by an independent authority.

European data protection certification covers only products, services and processes, not management systems. After consultation with the Swiss Accreditation Service (SAS), foreign data protection certification that meets the requirements of Swiss legislation is recognised. The FDPIC also recognises foreign certification bodies that meet Swiss requirements after consultation with the SAS.

In consultation with the Conference of Swiss Data Protection Commissioners (privatim) and the Federal Chancellery, the FDPIC has updated the guidelines for votes and elections, specifically in view of the upcoming federal elections in autumn 2023. These were published on his website in December 2022. In particular, the updated guidelines emphasise the critical importance of the data protection principle of transparency in voting and elections.

The guidelines were first drawn up in the reporting year 2018/2019 together with the Conference of Swiss Data Protection Commissioners (privatim) and in close consultation with the Federal Chancellery and a working group (see 26th Annual Report, Section 1.1). Since then, they have been updated on a regular basis (see 27th Annual Report, Section 1.1). In the year under review, they were structured more clearly, in particular, and extended to include the control questions formulated in the reporting year 2019/2020 regarding compliance with the data protection principles on websites.

approach

The FDPIC was able to present his concerns about the new E-ID Act during the office consultation on the bill. The draft legislation is expected in summer 2023.

In 2021, Swiss voters had rejected the first draft of the E-ID Act, demanding a new solution for a state-recognised digital identity (see 29th Annual Report, Section 1.1). In the year under review, the Federal Department of Justice and Police (FDJP) put forward a draft of the new E-ID Act (federal act on electronic identification services and trust infrastructure) for office consultation. The draft is based on the concept of a self-sovereign identity, allowing users the utmost control over their personal data.

All holders of an ID document issued by the Swiss authorities may apply to the latter for an e-ID. To this

end, the federal government will create and operate a state trust infrastructure which, on the one hand, will allow the e-ID to be checked for authenticity and, on the other, can be used by other public and private entities to issue and check other electronic proof. Accordingly, the first part of the bill regulates the state e-ID, while the second part regulates the trust infrastructure and other electronic proof. However, the bill does not regulate the details of the e-ID issuing process.

The FDPIC commented on the draft bill and was able to successfully present a number of demands. For example, the FDPIC was involved in developing provisions to restrict both the processing of metadata generated during use and the collection of data via the interfaces required for issuing the e-ID. As requested by the FDPIC, the draft E-ID Act also provides that

cantonal contact points are to be set up to provide assistance to citizens using the new e-ID. The FDPIC also stressed that it should be made clear in the dispatch on the bill that the e-ID should not result in citizens being required, as a rule, to identify themselves via the internet. With regard to the entities using the trust infrastructure to issue further electronic proof, the FDPIC demanded revocation obligations for issuers.

The FDPIC considers the proposed approach of an open register with fee collection to be problematic. With this system, people applying for an e-ID would enter their details in the register themselves, without their identity being verified beforehand. The FDPIC pointed out the associated risk of applicants with fake IDs abusing the trust infrastructure. In the FDPIC's view, the federal government should take measures to protect the infrastructure that it operates against unauthorised use. Therefore, we called for these risks to be made clear in the dispatch

to the Federal Council. We also pointed out that, if identities were not verified



beforehand, a system would be needed to confirm the identifiers present in the base register, as identifiers already in the

register could be linked to an individual, entity or organisation in the real world.

After considering the outcome of the consultations, the FDJP announced that it would define in greater detail the list of persons authorised to use the e-ID, the issuing process, data protection aspects, user-friendliness (including accessibility) and cantonal support services. The FDPIC will continue to monitor developments in this project and present his data protection concerns. The bill is to be submitted to the Federal Council by summer 2023.

Access with Swiss ID only from now on

In the year under review, Swiss Post outsourced the customer login process on its website, forcing users to use a SwissID to access its online services from December 2022 onwards. The FDPIC had been informed in advance and pointed out the requirements under data protection law.

When Swiss Post asked users of its online services to create a SwissID, we received numerous enquiries from members of the public about Swiss Post's actions.

The outsourcing of the login process and of the associated data processing to the private company SwissSign must not result in any disadvantage for Swiss Post customers with regard to their privacy or their right to informational self-determination.

Therefore, the FDPIC informed Swiss Post that the outsourcing of its login process to SwissSign was subject to the requirements of data processing by third parties in accordance with Article 10a FADP. Accordingly, Swiss Post remains liable to its customers for the data processing carried out by



SwissSign in connection with the login process on Swiss Post's website. Swiss Post was required to contractually guarantee

that SwissSign would ensure data security and process the data it collected from Swiss Post customers exclusively for the purpose of logging in.

After receiving assurances from Swiss Post that it acknowledged and agreed to comply with the data protection requirements for data processing by third parties with regard to the outsourcing of its login process, the FDPIC saw no need to take any supervisory action.

DIGITAL SWITZERLAND STRATEGY

Digital driving licence project

The Federal Roads Office (FEDRO), the Association of Road Traffic Offices (asa) and the Federal Office of Justice (FOJ) presented the digital driving licence project to the FDPIC. The FEDRO project is part of the Digital Switzerland Strategy.

The FEDRO is planning the phased introduction of a digital driving licence, provisional driving licence and vehicle registration document based on federal road traffic law. The digital documents will be recognised abroad and verifiable by police. They will be issued by the cantons in accordance with the form, content and design requirements laid down by the FEDRO.

The ID data is already stored in the driver registration information system (IVZ), which is jointly managed by the FEDRO and the cantons and which the cantons may access within the scope of their legal duties.

Based on the information he has received, the FDPIC feels that the project can be implemented in compliance with data protection regulations.

30 years of data protection

The Data Protection Act of 1992

The first Federal Act on Data Protection of 19 June 1992 came into force on 1 July 1993.

In its legislative dispatch of 23 March 1988, the Federal Council had already justified the need for legislative action based on the use of modern information and communication technologies in virtually all areas of life and the rapid intensification of data processing and its spread throughout society, the economy and government. Thirty years on, almost every aspect of our lives is digital, which legislators at the time could not have foreseen. Nevertheless, the principles of personal data processing enshrined in law at the time have proven timeless. The new Federal Act on Data Protection of 25 September 2020, which is due to come into force on 1 September 2023, is based on the same principles of transparency, proportionality and limitation of purpose, which remain the key pillars of personal data processing under the new law.

Although our everyday lives have been radically transformed by the internet and smartphones, many data protection issues remain as topical as ever. In our first Annual

Report, we already dealt with data processing by the police in the fight against organised crime and video border surveillance. Telephone monitoring and surveillance for law enforcement purposes were already being carried out at the time although nobody carried a telephone, camera, television, library or computer around with them in their pocket back then.

With today's digital society permanently connected to the internet as it goes about its daily business, from banking to online dating, the scope and intensity of personal data processing has grown exponentially. Nevertheless, the mission of the independent federal data protection supervisory authority remains the same, namely to prioritise people's fundamental rights and privacy over what is technologically possible. The current FDPIC has embraced this challenge, following in the footsteps of his predecessors, Odilo Guntern and Hanspeter Thür, who shaped the first 23 years of the federal data protection supervisory authority, and considers it a 'mission possible' despite the rapid pace of technological progress.

Old or new law - which applies?

Some proceedings could not be concluded in the reporting year. It is important to know here that, according to the transitional provision under Art. 70 new FADP, these will still be assessed under the currently applicable law, even if they are not concluded until after the new data protection law enters into force on 1 September 2023. This applies in particular to the clarification of the facts that the FDPIC opened in spring 2021 regarding the data processing of a Swiss online shop and the clarification of the facts regarding the data processing of the auction platform Ricardo AG and TX Group AG, both of which are still pending (s. 29th AR, Section 1.3).

The new Data Protection Act of 2023

The fully revised Federal Act on Data Protection of 2020 provides data controllers and the data protection supervisory authority with new instruments to meet the public's legitimate expectations in terms of robust protection of privacy in accordance with the rule of law. The FDPIC will thus intensify his supervisory activity.

The FDPIC's role

The new Federal Act on Data Protection will come into force on 1 September 2023. It introduces changes for data processors and data subjects and provides the FDPIC with additional duties and powers, who will thus intensify his supervisory activities and increase the number of investigations.

Institutional innovation

In future, the Federal Data Protection and Information Commissioner (FDPIC) will be elected by Parliament. Up until now, the FDPIC was elected by the Federal Council and was merely confirmed by the Federal Assembly. This new rule increases the office's independence from the executive and enhances its democratic legitimacy. The elected Commissioner recruits his own staff and has his own budget, the draft of which is still submitted to the Federal Assembly.

The FDPIC remains assigned to the Federal Chancellery for administrative purposes, especially since the FDPIC communicates with the Federal Council via the Federal Chancellor. The Federal Chancellery provides the FDPIC with a range of services in personnel administration, finance and office automation on the basis of a service level agreement.

From now on, it will be up to the Federal Council to decide whether or not the legislation of a third country provides adequate protection, allowing data to be transferred from Switzerland to that country without additional measures. A list of countries providing adequate protection will be annexed to the Data Protection Ordinance.

New duties for the FDPIC

If the planned processing of personal data is likely to involve a high risk to the privacy or fundamental rights of data subjects, private- and public-sector data controllers are required to carry out a data protection impact assessment (DPIA). If the DPIA shows that the planned processing still results in a high risk to the privacy or fundamental rights of data subjects despite appropriate measures being put in place, the data controller must seek a prior opinion from the FDPIC. The FDPIC will examine the DPIA and inform the data controller of any objections within two months. The FDPIC's opinion is not an authorisation to carry out the planned data processing. His opinion is not appealable but is subject to a fee.

The revised Act gives the FDPIC new duties. Professionals, industry and trade associations can draw up their own codes of conduct and submit them to the FDPIC for an opinion. The FDPIC publishes his opinions along with a list of standard data protection clauses that he has approved, issued or

"The FDPIC will intensify his supervisory activities and gradually increase the number of investigations." recognised. In future, the FDPIC will be able to charge fees for the opinions that he issues on codes of conduct and for the approval of standard data protection clauses and binding corporate data protection rules.

Under the revised Act, data controllers have a duty to report to the FDPIC any data breaches that may result in a high risk to the privacy or fundamental rights of data subjects. The FDPIC provides a reporting portal on his website for that purpose.

Investigations

As a supervisory body, the FDPIC is responsible for ensuring that federal bodies and individuals comply with the federal provisions on data protection, in particular the Federal Act on Data Protection (FADP). If there are sufficient elements to suggest that data processing may violate data protection regulations, the FDPIC will open an investigation, unless the violation is minor. In his investigation, the FDPIC determines the way in which a federal body or a private company or individual processes data relating to a natural person. On the basis of his findings, he will then assess whether or not there has been a breach of federal data protection regulations.

When the revised Data Protection Act comes into force, Switzerland will ratify the Council of Europe's Convention 108+. This is a legally-binding multilateral instrument on the protection of privacy and personal data that was opened for signature in 1981 and has recently been modernised to address the challenges of the digital age. In order to meet the requirements of Convention 108+, legislators have extended the investigative powers of the FDPIC. In the past, the FDPIC could only investigate the data processing activities of individuals in cases where the methods of processing were capable of breaching the privacy of a large number of individuals. This limitation ('system error') will no longer exist in the future.

The Commissioner will thus intensify the FDPIC's supervisory activities from the entry into force of the new law and gradually increase the number of formal investigations.

The authority has been provided with additional staff resources for the enforcement of the new law and was able to successfully complete the corresponding recruitments in spring 2023.

Informal preliminary investigations

Elements indicating a possible breach of data protection regulations may arise during ongoing supervisory activities or may be reported to the FDPIC by data subjects themselves or by third parties such as media companies or consumer protection organisations. If the FDPIC finds indications of a breach of data protection regulations, he begins by conducting an informal investigation to verify whether or not the matter is within his remit, whether there is sufficient evidence of a breach, and whether the breach is more than just a minor one. The FDPIC may informally ask the data controller to voluntarily answer questions if, for example, it is unclear whether the matter falls within his remit or if he believes that an investigation could be avoided by contacting the data controller. An investigation can be avoided, for example, if the data controller is able to immediately refute the existence of a breach or if they voluntarily take measures within a reasonable time frame to ensure compliance with the data protection regulations.

Formal investigation

Under existing law, a case investigation is carried out to establish the facts and to determine whether or not a breach of data protection regulations has occurred. After the investigation, if necessary, the FDPIC issues a legally non-binding recommendation that specific data processing activities be modified or suspended. Under the new law, investigations are governed by the Federal Act on Administrative Procedure (APA). If the FDPIC identifies a breach of data protection regulations during an investigation, he will have the authority to issue a legally binding order under Article 5 APA, which the data controller needs to challenge before the Federal Administrative Court if they do not wish to comply with it. The FDPIC may order that data processing activities be modified, suspended or discontinued, or that personal data be deleted.

Administrative assistance

The revised Act contains two provisions specifically regarding the FDPIC's cooperation with Swiss and foreign authorities. Swiss authorities are obliged to provide administrative assistance to the FDPIC, while the FDPIC has a duty to provide administrative assistance only to the Swiss data protection authorities, the law enforcement authorities in connection with his reports, and the federal authorities and police bodies involved in enforcing the measures ordered.

The FDPIC's administrative assistance to foreign authorities extends to data protection authorities. He may provide information and personal data required by the authorities for the performance of their respective statutory duties. A number of conditions need to be met, including reciprocal administrative assistance, confidentiality, and use of the information strictly for the proceedings in question.

Fees

In future, the FDPIC will charge private data processors for a number of his services. In addition to the activities already mentioned above that are subject to fees (opinions on codes of conduct and data protection impact assessments, and approval of standard contractual clauses and binding corporate data protection rules), the FDPIC will also charge fees

in the investigation procedure. In addition, he will charge private data processors for consultancy services. An hourly rate of between CHF 150 and CHF 250 will be charged depending on the position of the staff providing the service. Surcharges may apply if a service requires an extraordinary effort or is particularly difficult or urgent. The FDPIC may waive fees if the service is in the public interest or required little effort.

Criminal law

As before, unlike his EU counterparts, the FDPIC has no power to impose sanctions under the new law. However, the supplementary criminal provisions in the FADP have been extended. The wilful disregard of notification, disclosure and reporting obligations and the intentional violation of due diligence obligations are punishable. This applies in particular to the disclosure of personal data abroad, order processing and the provision of data security. Fines of up to CHF 250 000 may be imposed on the natural person responsible for the offence. Legal persons can be fined up to CHF 50 000, only as a subsidiary measure.

During the parliamentary consultations on the new FADP, the Federal Council announced that it would consider introducing administrative penalties for offending companies as part of a new federal act.

"The FDPIC can now order that a data processing operation be terminated or that personal data be deleted."



DPIA

REPORTING PORTALS

The FDPIC advises the FOJ on guidelines for data protection impact assessments within the Administration

Under the fully revised Federal Act on Data Protection (nFADP), the offices of the Federal Administration are required to perform a data protection impact assessment (DPIA) before they carry out any data processing which is likely to result in a high risk to the privacy or fundamental rights of the individuals concerned. The FDPIC advised the Federal Office of Justice (FOJ) on guidelines and tools for the federal bodies.

When planning projects for the digital transformation of the Federal Administration, the offices responsible need to assess the potential risks to the privacy and fundamental rights of the individuals concerned. If the planned processing of personal data is deemed likely to result in a high risk, the federal bodies in question are required to perform a data protection impact assessment in which they identify the risks and the measures needed to mitigate them.

The FDPIC helped the FOJ to formulate guidelines and tools to facilitate the work of the federal offices in this respect. The FDPIC stated that it was important not to rely solely on (software-assisted) aids and final checklists both in the preliminary examination aimed at identifying the need for a DPIA and in the DPIA itself. A DPIA requires an evaluative assessment of the overall risk, taking into account all aspects of the specific case at hand. Based on practical experience with risk assessments carried out by the Federal Administration under the current Schengen Data Protection Act, the FDPIC also pointed out that under the DPIA guidelines, federal bodies should report any significant changes in their existing data processing operations compared with their planned activities. The comparison should include systemic aspects (scope, frequency and duration of data processing as well as access rights) as well as security aspects of data processing.

Reporting portals for the new Data Protection Act

In the run-up to the entry into force of the new Federal Act on Data Protection, the FDPIC has introduced new reporting portals, one of which is already available, namely the portal for federal bodies to register their data processing activities. A portal for registering data protection officers and one for reporting data security breaches will follow.

In 2021, the FDPIC launched a project for the creation of three reporting portals.

With the introduction of the new record of processing activities for federal bodies provided for in Article 12 nFADP (DataReg) replacing the current system for registering private and official data files (WebDataReg), we were able to launch the first reporting portal in November 2022. The completely redesigned DataReg is used for registering and publishing records registered by the federal bodies and is intended to help the authorities manage them. The current portal (WebDataReg), which is also used to publish the data files of private companies, will be discontinued on 1 September 2023. Under the new law, the latter are no longer subject to registration.

The reporting portal for data protection officers is for registering the contact details of appointed data protection officers.

The portal for reporting data security breaches under Article 24 nFADP (Data breach) provides a secure digital channel for data controllers to report data security breaches that pose a high risk to the data subjects concerned. The online form helps data controllers enter all the required data in a structured manner and is intended to help the FDPIC process reports efficiently and to facilitate statistical analysis.

1.2 Justice, Police, Security

FOCBS

Customs Act

The draft comprehensive revision of the Customs Act is currently being discussed by the Parliament's Economic Affairs and Taxation Committees. In this context, the FDPIC was heard by the National Council Committee. In particular, he pointed out the sensitive nature of the project and the disproportionate access to the information system of the Federal Office for Customs and Border Security (FOCBS) granted to the Federal Intelligence Service.

On 24 August 2022, the Federal Council submitted to Parliament a draft federal act on the general provisions governing the collection of levies and control of the cross-border movement of goods and persons by the Federal Office for Customs and Border Security (act setting out implementation by the FOCBS). The National Council Economic Affairs and Taxation Committee is in charge of reviewing the bill and interviewed the FDPIC on 24 October 2022.

The merger of police and customs operations within the FOCBS has posed a challenge to the Confederation in terms of data protection supervision. The creation of a new customs police office has increased the number of persons processing personal data under both customs and police law. The standardisation of the customs administration has created a third major security authority at federal level in addition to the Federal Office of Police (fedpol) and the Federal Intelligence Service (FIS).

As mentioned in our 28^{th} Annual Report 2020/21 (see Section 1.2), the Federal Department of Finance initially submitted a bill for consultation that was unacceptable from the point of view of federal data protection supervision. The bill did not specify how

the customs police office would process personal data, leaving this to the discretion of FOCBS managers.

As part of our intensive and longterm support, in agreement with the Federal Office of Justice, we have en-



couraged the FOCBS to draw up a comparison between the current processing of personal data by the FCA and future

processing by the FOCBS. This comparison has been included in the data protection impact assessment. On this basis, the FOCBS has revised and clarified in detail the section on data processing (see 29th Annual Report 2021/2022, Section 1.2). In the meantime, with these improvements in place, the FDPIC's fundamental objections raised during the third office consultation were withdrawn, as a result of which the bill submitted to Parliament is now acceptable from a data protection perspective.

Despite the improvements made, however, the draft FOCBS enforcement remit act is to be regarded as sensitive under data protection law. During the PROTECTION STATUS S

third and final office consultation procedure, the new proposal to grant the FIS access to the FOCBS information system remained controversial. The current Customs Act does not provide for such access, as sporadic cooperation between Customs and the FIS can take place on a case-by-case basis within the framework of mutual administrative assistance. The insistence on granting access shows that the Confederation's three major security authorities are keen to intensify the processing of personal data by granting each other unrestricted access to their respective information systems. The Federal Council has maintained FIS access in the act despite the fact that we consider it unnecessary and therefore disproportionate.

Web application RegisterMe

The State Secretariat for Migration (SEM) has set up a web application for refugees to apply for protection status S. The FDPIC expressed security concerns over the storage of personal data of this vulnerable group and welcomes the action subsequently taken by the SEM. Tens of thousands of people who have entered Switzerland after being forced to flee the war in Ukraine have applied to the State Secretariat for Migration (SEM) for temporary protection (protection status S). The web application RegisterMe is used for booking an appointment for registration at a federal asylum center and was introduced as a fast-track system for processing the large number of applications and appointments.

The FDPIC had already identified potential risks to the data subjects' personal data just a few days after RegisterMe was launched and raised his security concerns with the SEM. He

had also noticed that there was no way to delete the registration details of these vulnerable individuals in the web application. He therefore advised the SEM to introduce a way to delete the data and to delete it immediately after the appointment. Specifically, he advised the SEM to create and implement a deletion method.

The SEM now uses two-factor authentication to protect the personal data, which is stored at a computer center specially designed for the storage of sensitive data. Furthermore, the SEM has introduced a method for deleting the data, which was implemented in September 2022.

MITTO AG

Preliminary clarification on possible misuse of the 'signalling system access'

In December 2021, international media coverage drew the FDPIC's attention to allegations of unlawful data processing by an employee of the Zug-based company Mitto AG. A preliminary investigation found no evidence of a breach of data protection regulations. The FDPIC has concluded his preliminary investigation with a final report, without issuing any recommendations.

In December 2021, following media coverage, the Federal Data Protection and Information Commissioner was alerted by an article published by the Bureau of Investigative Journalism and Bloomberg News to allegations of unlawful data processing by an employee of the Zug-based company Mitto AG. The article alleged that the

employee in question had abused the access granted by mobile phone operators to their networks for the purpose



of sending text messages to obtain information for other purposes. In particular, the employee allegedly used access to the

signalling system (SS7) to enable the unauthorised surveillance of individuals in return for payment (see 29th Annual Report, Section 1.3).

The FDPIC demanded detailed information from Mitto AG in several stages on the technical and organisational safeguards in place at the company. Mitto AG complied with all of the FDPIC's requests and conducted its own external investigations, the results of which were shared with the FDPIC.

Mitto AG produced documentation on the organisational framework of its operations and described the measures in place to prevent and detect unauthorised changes to the software. According to Mitto AG, the logging data showed no evidence to suggest that the systems had been abused in the manner alleged.

According to Mitto AG, and confirmed by mobile operators in Switzerland, who were also invited to comment, it is impossible for Mitto AG employees to access the location data of SMS recipients without modifying the systems or software.

The FDPIC has carried out all the necessary inspections that were possible with the resources available to him but no evidence has come to light confirming that a breach of data protection regulations has taken place.

In view of the foregoing, the FDPIC has decided to conclude the preliminary investigation into Mitto AG without making any recommendations.



1.3 Commerce and economy

DISCLOSURE OF PERSONAL DATA TO FOREIGN TAX AUTHORITIES

The Federal Supreme Court rules against the right to information of third parties in international administrative assistance in tax matters

In 2019, the Federal Administrative
Court upheld an objection by the FDPIC
concerning the right to information of
third parties in international administrative assistance in tax matters. In the
subsequent appeal procedure before
the Federal Supreme Court, the Commissioner once again defended this
right of third parties. In December 2021,
the Federal Supreme Court upheld the
Federal Tax Administration's objection
following a change in practice that had
occurred in the meantime and overturned the ruling by the Federal Administrative Court.

In international administrative assistance in tax matters, the right to be informed about ongoing administrative assistance proceedings is linked to the right to appeal (see Article 14 of the Tax Administrative Assistance Act). In 2017, the FDPIC issued a recommendation that, in international administrative assistance in tax matters, the Federal

Tax Administration (FTA) should also notify in advance any persons who were not affected by the request for administrative assistance (i. e. third parties) but whose names were to be disclosed in unredacted form to the requesting foreign authority (see 25th Annual Report, Section 1.9.2). In the FDPIC's opinion, third parties were entitled to oppose the unlawful disclosure of their data by lodging an appeal. The FTA rejected this recommendation, prompting the FDPIC to take the



matter all the way to the Federal Administrative Court (see 26th Annual Report, Section 1.3). In its ruling of 3 September 2019,

the latter concluded that in international administrative assistance in tax matters, in principle, persons who were not affected by the request for administrative assistance (third parties) but whose data was to be transmitted in unreducted form needed to be notified in advance. Exceptions need to be provided for, namely cases in which notification would require disproportionate effort, thus rendering the provision of administrative assistance impossible or causing disproportionate delays. The FDPIC welcomed the ruling as it protected the fundamental rights of bank employees and other third parties.

The FTA appealed the decision before the Federal Supreme Court. The latter lifted the suspension of proceedings requested by the FTA after delivering a landmark ruling (BGE 146 I 172) in another matter on 13 July 2020. In the ruling in question, the Federal Supreme Court severely restricted the right to information, stating that third parties whose data was to be disclosed by the FTA to a requesting foreign authority in unredacted form were entitled to appeal only by way of exception, namely in special circumstances. This means that the FTA is not required to notify ex officio all third parties entitled to appeal before their details are disclosed but only those who are clearly entitled to appeal on the basis of the files.

In light of this ruling, the FDPIC recognised before the Federal Supreme Court that, in international administrative assistance in tax matters, third parties were entitled to appeal only by way of exception. However, he reiterated the view expressed by the Federal Administrative Court that, in principle, all third parties should be notified in advance ex officio before their personal data is disclosed. Only that way can all third parties who are entitled to appeal

TRACKING TECHNOLOGIES

in accordance with the Federal Supreme Court ruling exercise their right to do so and oppose the disclosure of their data. The FDPIC then outlined again before the Federal Supreme Court how the FTA could fulfil a fundamental duty of notification without requiring a disproportionate effort that would render impossible or excessively delay the provision of international administrative assistance in tax matters (see 28th Annual Report, Section 1.3).

In its ruling of 21 December 2021 (BGE 148 II 349), the Federal Supreme Court reaffirmed the case law established by the aforementioned ruling BGE 146 I 172, according to which the FTA was required to notify third parties ex officio before disclosure of data only if the parties in question were clearly entitled to appeal on the basis of the files. Contrary to the FDPIC's interpretation, the Court found that this was expressly regulated in Article 14 paragraph 2 of the Tax Administrative Assistance Act. The Federal Supreme Court rejected a general obligation of advance notification based on Article 18a paragraph 3 FADP, pointing out that the disclosure of data relating to third parties was expressly regulated in the Tax Administrative Assistance Act. It therefore upheld the FTA's appeal and overturned the Federal Administrative Court ruling of 3 September 2019.

Investigation into a possible breach of Swiss people's right to privacy by Oracle

The FDPIC learned of a US lawsuit filed in August 2022 against Oracle America Inc. in which US plaintiffs raised serious allegations of unlawful tracking of internet users. The case is currently being reviewed to determine whether the allegations raised also affect people in Switzerland.

The US lawsuit accuses Oracle America Inc. of using tracking technologies to collect data on 5 billion internet users and compiling it in a database. Oracle allegedly analyses and evaluates the data it collects in order to create a file

on each of the data subjects. As well as names and addresses, the company



allegedly records all types of internet activity, for example purchasing behaviour, GPS data and health information, even

across devices. The lawsuit claims that Oracle tracks internet users by means of various technologies, in particular cookies and pixels, as well as JavaScript code embedded in websites and apps. The lawsuit is still pending, with the US court yet to rule on the allegations raised.

The FDPIC is reviewing the allegations made in the lawsuit to establish whether there have been any breaches of privacy for people in Switzerland. He has contacted Oracle Software (Switzerland) GmbH but the technical aspects are proving to be complex, as a result of which no formal investigation has yet been opened.

30th Annual Report 2022/23

POSTFINANCE

Waiving account publicity

Following the FDPIC's demand that PostFinance offer an opt-out option for account holders who did not want their account details to be publicly accessible, the auto-completion of account details on the e-banking platform is expected to be reduced in the future to a level that is customary in the industry.

During the last reporting year, we conducted a preliminary investigation into the auto-completion of account details on PostFinance's e-banking platform (publicly accessible account details). This came after members of the public alerted us to the fact that the PostFinance e-banking portal provided access to the details of any number of account holders as the system automatically added the name and address of the account holder associated with the account number entered in the payment entry form (see 29th Annual Report 2021/2022, Section 1.3). After



PostFinance took measures to prevent mass queries on its e-banking portal, we demanded that custom-

ers be offered the chance to opt out from their account details being made publicly accessible and being completed automatically.

PostFinance looked into the possibility of implementing such an opt-out and then decided not to make account details publicly accessible in the future. According to PostFinance, in the future only account details that users have already entered for a previous payment order will be automatically completed on its e-banking platform, in line with customary industry practice. The necessary changes are expected to be made by the end of 2023. We will check to ensure that these measures are implemented.

CREDIT-HISTORY CHECKS

Database entries based on poor household credit history

The FDPIC has concluded his case investigation at a debt collection and credit-rating agency. He found the use of 'poor household credit history' to be inadmissible.

In the reporting year 2019/2020, the FDPIC initiated a procedure against a large debt collection and credit-rating agency after it was alleged that its database contained too many incorrect entries, resulting in individuals with the same or similar names being confused with one another. The mix-ups meant that payment reminders were being sent to the wrong persons, and incorrect poor credit histories were being stored and made public. The FDPIC also looked at how easy it was to correct any incorrect entries. The scope of the investigation was then extended to assess the admissibility of the company's use of 'poor household credit history' (see 27th Annual Report, p. 37; 28th AR, p. 34, and 29th AR, p. 39).

Anyone who processes personal data must make certain that it is correct



(Article 5, paragraph 1 FADP). Mix-ups due to incorrect database entries regularly lead to invasions of personal privacy which

can sometimes severely impact the individuals concerned. After a thorough examination, the FDPIC concluded that the company under investigation complied with the data protection requirements regarding measures implemented to ensure the accuracy, upto-dateness and completeness of the data. However, even when data is processed carefully and the necessary measures are taken, incorrect database entries may still occur. Therefore, it is important that data is processed in a manner that is transparent for the data subjects and that an effective correction and deletion process is in place to avoid the negative impact of incorrect database entries. The company under investigation was found to meet these requirements as well.

As part of his investigation, the FDPIC also assessed the admissibility of disclosing 'poor household credit history' within the context of credithistory checks. What this means is that when a person's credit history is checked, any poor credit history of other persons in the same household is disclosed. The company explained that this disclosure of data - for example to online retailers - was intended to prevent individuals with a poor credit history from being able to make purchases on account under the name of a household member with a good credit history (known as 'evasive transactions'). As a result of this practice, the credit histories of household members

become linked so that individuals with a good credit history are themselves no



longer able to make on-account purchases. In his investigation, the FDPIC concluded that this processing practice violated

the principles of transparency and proportionality set out in the Federal Act on Data Protection. The processing of data in this way cannot be justified. In particular, the overriding interest justifying a credit-history check (Article 13 paragraph 2 letter c FADP) does not apply because the poor credit history of another household member cannot be considered decisive for establishing the credit history of a person entering into a contract. For these reasons, the FDPIC recommended in his final report that the company stop providing credit information based on 'poor household credit history'.

The company has accepted the recommendation.

CYBER ATTACK

Preliminary investigation into Infopro AG and Fiducial Winbiz SA

The FDPIC launched a preliminary investigation following a cyber attack on a Swiss cloud hosting service provider. He assessed the action taken and informed the parties concerned of their data protection obligations.

In late November 2022, it was reported that the hosting company Infopro AG had suffered a cyber attack. Among other things, the company processed personal data on behalf of Fiducial Winbiz SA, a provider of cloud-based management and accounting software widely used in the French-speaking part of Switzerland. As a result of the cyber attack and subsequent action taken, some business customers had temporarily lost access to the cloud application and the personal data stored in the cloud.

The FDPIC received numerous enquiries from Infopro SA's business customers regarding the cyber attack and advised them on the matter. Where personal data was involved, he reminded customers of their obligations to inform the data subjects and to mitigate the data protection risks. The companies concerned made every effort to fulfil their obligations within a very short time.

The FDPIC contacted Infopro and Winbiz to promptly establish the facts, in particular to investigate the allegations of a security flaw in the Winbiz

PRELIMINARY INVESTIGATION AT A VOICE SERVICE PROVIDER

DATING-APPS

software that is thought to have allowed customers to access the data of other customers. The FDPIC sent Winbiz a



questionnaire, inviting it, in particular, to comment on the reported violation of access restrictions. Infopro was also sent a ques-

tionnaire. Meanwhile, discussions have taken place with the cantonal data protection authorities (privatim) and with the National Cyber Security Centre (NCSC), which works alongside the competent prosecution authorities.

Based on the answers received, the FDPIC was able to establish that both companies had taken the necessary action to restore control over the personal data and had notified the customers concerned. The alleged security gap was not confirmed, and so the FDPIC saw no need for any further action for the time being. Nevertheless, he asked Infopro and Winbiz to keep him informed of any developments.

Security vulnerability promptly fixed

The FDPIC carried out a preliminary investigation at a voice service provider after being alerted to a security vulnerability. The provider took immediate remedial action, so the FDPIC did not need to initiate formal proceedings. In the year under review, the FDPIC was alerted by a journalist and a member of the public to the fact that personal data could be freely accessed via the website of a voice service provider. A large number of recorded telephone conversations could be easily accessed without a password, and in some cases the data included additional information that made it easy to identify specific individuals.

As a result, the FDPIC opened an informal preliminary investigation at the voice service provider in question. The company pointed out that it had promptly fixed the vulnerability, investigated the security incident and implemented additional security measures. The FDPIC only needed to make a few suggestions for improvement, which the service provider implemented. Given the circumstances, the FDPIC saw no reason to launch a formal case investigation and therefore closed the preliminary investigation.

Analysis of the data processing

In the reporting year, the FDPIC sent his final report to a Swiss-based dating app provider that operates internationally. He also made recommendations, which have been accepted.

In spring 2021, the FDPIC launched an investigation into the data processing activities of a dating app. In particular, he wanted to check whether the handling of deletion requests and the disclosure of personal data to third parties complied with data protection regulations and to verify compliance with transparency and data security requirements (see 28th and 29th Annual Reports, Section 1.1 in both cases).

The FDPIC's investigation concluded that although deletion requests were processed within a short period of time, the overall deletion concept was inadequate. Users were also provided with insufficient and misleading information regarding deletion options. The information about the data processing carried out when using the

VIRTUAL RACES

app was deficient, particularly with regard to which data are being processed for which purposes. The FDPIC made several recommendations to remedy these shortcomings and to ensure compliance with the processing principles of transparency, proportionality, good faith and lawfulness.

The app provider uses third-party applications to perform various functions on the app instead of developing its own applications. In doing so, the provider transfers the processing of personal data to the third-party service providers. In the FDPIC's judgment, the app provider did not take the necessary measures as the data controller (e.g. clarifications and agreements) to ensure that these service providers only processed the data as requested and in accordance with data protection law. Furthermore, the app provider only carried out internal security tests, which does not meet data security requirements given the sensitivity of the data being processed. In light of this, the FDPIC made recommendations intended to strengthen data security and ensure that the outsourcing complied with the law.

The app provider has accepted all of the recommendations. Once all of the recommendations have been put into practice, the FDPIC will be able to conclude the investigation.

Improved data protection at a virtual race organiser

The FDPIC was notified of data protection issues at an organiser of running events. In response, he opened a preliminary investigation and contacted the organiser. The latter took prompt action to improve data protection so that the FDPIC saw no need to launch a formal investigation.

A company provides an app enabling runners to compete against each other in virtual races. The runs are time-in-dependent (i. e. a given route can be completed at any time within a specifiable time frame) and, depending on the event on offer, location-independent (i. e. you can run wherever you want). Runners are then ranked according to their results. Of concern was the fact

that the web development tool could be used to collect the ranking data of numerous individuals with just a few



clicks and that that aspect was not clear to the data subjects. After an exchange with the FDPIC, the operator clarified its

privacy policy and incorporated it in its registration process. Moreover, it removed the 'place of residence' parameter from its rankings, making it hard to identify individuals. We also found that users were able to choose a pseudonym when registering for a virtual run but that many people deliberately entered their real first and last names. Users can also delete their ranking information themselves.

This informal exchange with the FDPIC enabled the race organiser to improve the level of data protection immediately so that the FDPIC saw no need to launch a formal investigation.

30th Annual Report 2022/23



1.4 Health

NATIONAL ORGAN DONOR REGISTER NODR

Online authentication unsufficient

The investigation into the national organ donor register has been concluded, and the final report has been published on the FDPIC's website. This case highlights the importance of having reliable online authentication processes in place. Easy-to-use authentication solutions are widely available.

In 2022, the FDPIC conducted and concluded an investigation into the national organ donor register operated by the Swisstransplant Foundation. This online register was designed to allow citizens to register their willingness or refusal to donate organs after death. This information constitutes sensitive personal data within the meaning of Article 3 letter c number 2 FADP as it reveals intimate aspects of an indi-



vidual's life. The investigation had been launched after media reports revealed flaws in the registration process that made

it possible to register another person without their knowledge. The investigation was carried out in various stages:

 The FDPIC submitted a first report to Swisstransplant in mid-June in which he issued a number of recommendations regarding the implementation of more reliable user authentication processes for registration, subsequent logins, and changes to data in the register;

- · Swisstransplant commented on the report in summer 2022. In particular, the foundation stated that it would not be putting the register back online with its full functionality: the register would only remain available for consultation but would no longer allow new registrations or changes to existing profiles, allowing only deletion. This decision made some of the FDPIC's recommendations redundant, namely those aimed at improving the authentication processes for online registration. In addition, Swisstransplant accepted most of the other recommendations, with the exception of two concerning a residual risk associated with the deletion of profiles;
- The FDPIC submitted his final report in mid-October. Shortly thereafter, Swisstransplant announced its decision to permanently cease operation of the register. The register was effectively closed in December 2022 and all the data deleted.

In this context, it should be noted that in the referendum of 15 May 2022, Swiss voters accepted the principle of presumed consent for organ donation and the creation of a register maintained by the Confederation, with a function similar to that of the register operated by Swisstransplant. The new register is due to be launched in 2025.

Online authentication tools

The case of the Swisstransplant register is a prime example of just some of the pitfalls of operating an online register. Such a tool is undoubtedly very practical as it can be consulted remotely and allows users to manage their own profiles. Simple registration and profile management processes are typically favoured for accessibility purposes. That said, there is a risk of over-simplification, which opens the door to improper use by malicious individuals (identity theft, hacking, chicanery etc.). Operators of registers should be aware that they are responsible for ensuring the accuracy and security of the data in their register, especially if the latter is intended to support decisions made by

others, for example family members or doctors, regarding organ donation. It should be pointed out that reliable and easy-to-use online authentication tools are available and widely used, particularly in the banking sector. There are also various e-ID solutions already available. When considering setting up such a register with online authentication, it is important to do the necessary research beforehand in order to choose secure solutions. Digitalisation opens up a wealth of new opportunities for healthcare but also introduces additional risks. It is in the interest of operators in the sector to maintain a high level of user confidence by implementing robust and reliable digital solutions.

30th Annual Report 2022/23

ONLINE REGISTERS

Data protection risks in the breast implant register

The case investigation into the breast implant register has been completed. This case illustrates that providing online access to medical information inherently carries additional risks. Therefore, the question needs to be asked whether the additional risk is necessary. If so, adequate resources need to be allocated to ensure data security.

In 2022, the FDPIC launched a case investigation into the breast implant register managed by the Swiss Plastic Surgery Association (see 29th Annual Report, Section 1.4). The register records all breast plastic surgery operations involving implants along with any difficulties encountered during the operations and serves several purposes. On

the one hand, it aims to improve the quality of service by sharing information on any incidents. It also allows the tracking of implants to facilitate product recalls in the case of defects found in a series of implants. On the other hand, the data collected is also used for the compiling of industry statistics.

The FDPIC launched an investigation after a flaw was reported in the register's IT architecture that allowed anyone to access patient records in a few simple steps. In addition to personal details (first name, last name, date of birth etc.), medical information regarding operations was also accessible. The FDPIC is currently preparing his report, which is due to be completed later this year. Meanwhile, the register has been taken offline.

Balancing needs and risks

This case highlights another sensitive aspect of online medical registers. The information they contain is by definition highly sensitive as it relates to people's health and is often very personal.

Making this information available online inevitably exposes patient data to significant risks and can potentially damage the relationship of trust between doctor and patient. This data is regularly sent by doctors themselves, who are bound by professional secrecy, subject to the prior consent of the patient. Furthermore, one must always ask whether the purpose of the register justifies the risk taken and which data



is absolutely essential in order to achieve the intended purpose, in accordance with the principle of proportionality

enshrined in Article 4 paragraph 2 FADP. If so, the operators of such registers must take adequate measures and allocate sufficient resources to address the risks.

LACK OF DATA SECURITY

Investigation into database of private Covid-19 test centers

The FDPIC conducted an investigation into a database of private Covid-19 test centres that presented security issues. In his final report, he pointed out that the data was exposed to significant security risks due to a known vulnerability. However, the data controllers promptly took appropriate action when the flaw was detected, minimising the risk to the data subjects, so that the FDPIC was able to close the investigation without the need to issue any recommendations.

In November 2022, the FDPIC and the NCSC were alerted by a member of the public to a data security issue concerning a database containing the results of Covid-19 tests conducted in various centres across Switzerland. Due to a vulnerability in the web server used to access the database, the person in question had managed to access the database using information contained in a freely accessible configuration file and download a copy of the database. The data controllers took the database off the server the very day the vulnerability was reported and transferred it to an encrypted physical data carrier.

After learning about the case and conducting initial inquiries, the FDPIC opened an investigation, during which he identified various security deficiencies. The configuration file had become freely accessible following system

maintenance, which represented a critical vulnerability as it contained access data enabling unauthorised



persons to access the database. In addition, the authentication method used, involving a username and password (both

of which were contained in the exposed file), was found to be inadequate in the given context: two-factor authentication, for example, should have been used to ensure data security.

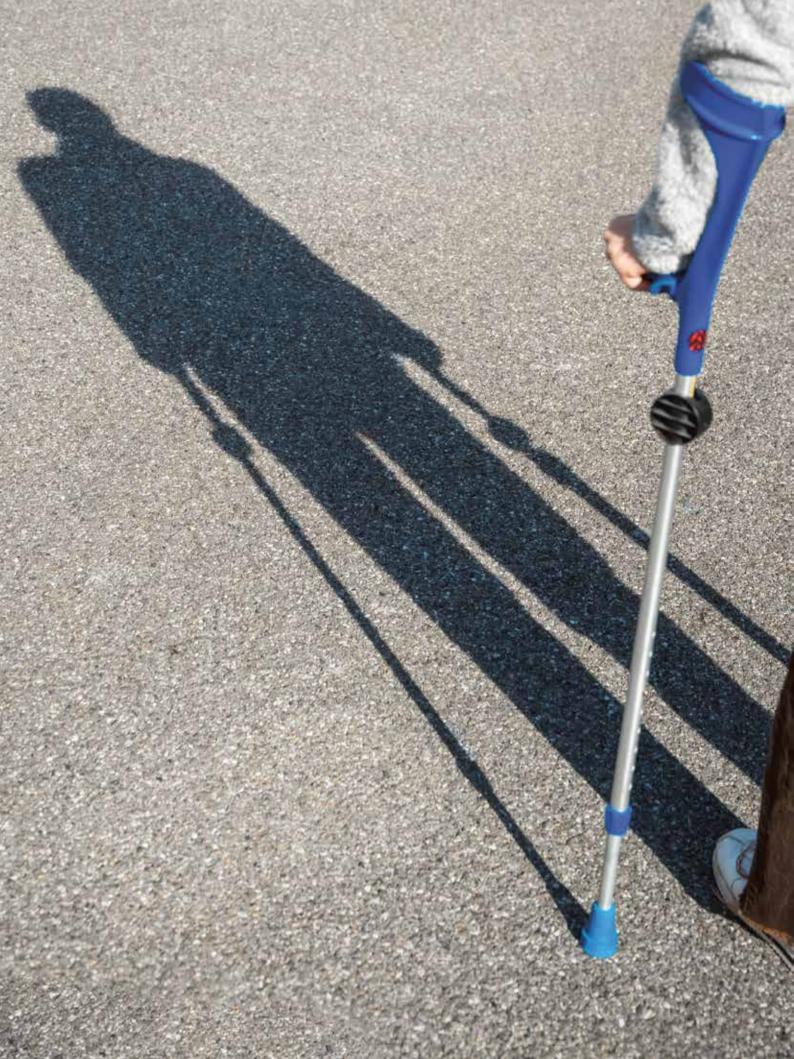
As the system was also used abroad, the FDPIC sought administrative assistance from the data protection authorities of Austria and the Principality of Liechtenstein.

From the access logs, the responsible of the test centres was able to confirm that there had been no further unauthorised access to the data. Moreover, the prompt action taken had eliminated all risks to the data subjects. Due to the specific circumstances of the case and the fact that the Covid test centres had already ceased operation some time before the vulnerability was detected, the FDPIC closed the investigation without issuing any recommendations.

Growing number of cases involving ethical hackers

In addition to the growing number of investigations conducted by journalists into data protection and security gaps, the FDPIC is increasingly receiving reports from ethical hackers, or 'white hat hackers', and IT activists. White hat hackers like to think of themselves as well-intentioned and will typically report cases to the FDPIC in the hope that he will take up the issues with the operators and, if necessary, investigate. They act outside an official framework and without the consent of the system operators, often gaining access to personal data (for example customer or employee data).

It should be noted that, as well as reporting their discoveries to the FDPIC, as in the case of the Covid test centre, these hackers sometimes inform the public or the media directly. Depending on the information provided, disclosing it in this way can generate additional risks for the data subjects concerned.



ONLINE PLATFORM

Project to recover vaccination data of meineimpfungen.ch platform

At the end of 2021, the former operator of the meineimpfungen.ch platform was declared bankrupt. In May 2022, the FDPIC learnt that the bankruptcy office in charge was planning to sell the vaccination data to a private company, which prompted him to recommend that the data be deleted instead. In response, the authorities and members of the public demanded that the data be recovered. In June 2022, under a public-law agreement called for by the FDPIC, the Canton of Aargau took over the data, as part of a preliminary project that is still ongoing, in order to examine the possibility of returning the data to the data subjects in a manner compliant with data protection regulations.

In 2021, serious deficiencies were identified on the meineimpfungen.ch platform, and unsuccessful attempts were made to enable the data subjects to



access their data in compliance with data protection regulations. At the end of 2021, the platform operator was declared

bankrupt (see 29th Annual Report, Section 1.4), and in May 2022, the FDPIC learnt that the vaccination data in question was to be sold to a private

company as part of the bankruptcy proceedings. After consulting the data protection commissioner of the Canton of Bern, the FDPIC intervened by issuing a formal recommendation on 20 May 2022 to the bankruptcy office acting on behalf of the bankrupt operator prohibiting the sale and demanding that all vaccination data be deleted from the platform. The bankruptcy office accepted the recommendation.

Following the FDPIC's recommendation, several authorities, including the Federal Office of Public Health (FOPH), and members of the public publically requested that the data be recovered and returned to the data subjects. In response to the public interest expressed in recovering the data, the FDPIC wrote to the head of the FOPH in June 2022 declaring that he was willing to revoke his call for deletion of the data on condition that the data be transferred to a federal or cantonal health authority on the basis of a publiclaw agreement in order to safeguard

the data subjects' privacy rights (this purpose was to be expressly stated in the agreement).

On 16 June 2022, the bankrupt operator, represented by the Bern-Mittelland Bankruptcy Office, concluded an agreement to that effect with the Canton of Aargau, supported by the FOPH. As a result, the FDPIC was able to revoke his recommendation of 20 May 2022. The data was then transferred to the Canton of Aargau and the reference community eHealth Aargau (acting on behalf of the canton) in accordance with the agreement so that a preliminary project could be carried out to determine whether or not the data could be returned to the data subjects in a manner compliant with data protection regulations. As well as focussing on ensuring data integrity, the project would assess the technical and economic feasibility of the plan and the possibility of transferring the data to an electronic patient dossier, whereby explicit consent would be required in each individual case. If the project proves unviable, the Canton of Aargau, the reference community and the FOPH have agreed that it will be terminated and the data deleted.

At the time of going to press, the outcome of the preliminary project of the Canton of Aargau, carried out under the supervision of the cantonal data protection commissioner, was not yet known.

30th Annual Report 2022/23

ELECTRONIC PATIENT RECORDS

New developments

During the year under review, the Federal Department of Home Affairs (FDHA) submitted a consultation draft to the Federal Council to guarantee transitional funding of electronic patient records (EPRs) in the form of financial support until the law is revised. A complete revision of the Federal Act on the Electronic Patient Record (EPRA) to ensure the successful introduction and use of EPRs is expected to be submitted for consultation in summer 2023.

At its session on 27 April 2022, the Federal Council decided to develop the EPR further through a variety of measures and instructed the FDHA to prepare a consultation draft taking into account a number of specific key points. The fully revised EPRA is due to be submitted for consultation in summer 2023 and is not expected to come into force before 2027. The Federal Council wants to see EPRs become an integral part of the compulsory health insurance system, which will give the Confederation broad regulatory powers. However, insurance companies will not have access to EPRs.

Tasks and responsibilities and, therefore, guaranteed EPR funding by the Confederation and the cantons are clearly defined. With regard to the voluntary nature of patient participation, two variants are to be submitted for consultation: keeping participation voluntary, and introducing an opt-out



model, whereby the Federal Council favours the latter. All healthcare professionals working in the outpatient sector are

obliged to use EPRs. Newly licensed physicians have been required to do so since I January 2022. With the consent of patients, researchers are to be granted access to EPR data. To facilitate processing, the dynamic data is to be stored centrally. The technical infrastructure of the EPR may also be used for additional services such as patient referral to other healthcare professionals. The use of an e-ID to access EPRs has yet to be clarified.

In order to secure EPR funding until the EPRA has been revised, the Federal Council has instructed the FDHA to submit for consultation a bill on transitional EPR funding by spring 2023. The bill will then be submitted to Parliament and will need to come into force within the shortest possible time frame. The Federal Office of Public Health (FOPH) has begun work on the two revisions.

Furthermore, as part of the annual revision of the implementing provisions of the EPRA, the FOPH and eHealth

Switzerland are examining other ways in which the EPR needs to be developed further and updated, to be implemented in spring 2023. The above-mentioned revision projects are intended to promote the use and dissemination of EPRs, in particular by including an electronic vaccination record and a national electronic medication plan. Various ways of making the EPR more attractive are also being assessed.

The FDPIC holds regular discussions with the FOPH and gives regular opinions on its projects. He has repeatedly stressed that he is not opposed to facilitating the rollout of the EPR in the interest of patients but that this should not lead to a relaxation of data protection requirements. He will continue to monitor developments on the EPR closely and remains committed to ensuring data protection, particularly where the measures envisaged impact data subjects' right to privacy or if there are plans to make EPRs compulsory for all patients.

Legal obligation to send copies of medical invoices

The obligation of service providers to send policyholders copies of their medical invoices has raised a lot of questions, comments and uncertainty among policyholders, particularly regarding privacy and security concerns associated with electronic transmission.

As of 1 January 2022, all service providers within the meaning of Article 35 paragraph 2 of the Swiss Federal Health Insurance Act (KVG/LAMal), namely physicians, pharmacists, chiropractors, hospitals, laboratories etc., are legally required to send policyholders a copy of their invoice in all cases and without the latter having to request it. With the express consent of the policyholder, the copy may be sent electronically. The obligation to send copies to policyholders was adopted with the amendment of Article 42 paragraph 3 of the Federal Health Insurance Act as part of a package of measures designed to control healthcare costs more effectively. The aim is to allow policyholders to check their invoices and report any errors to the insurance company. This obligation is not new as it already existed in the third-party payer system but had previously been regulated only at ordinance level.

In this regard, the FDPIC contacted the Federal Office of Public Health (FOPH), the office responsible for implementing the measure, to ensure that service providers are well informed of their obligations, particularly with regard to privacy and security requirements when sending copies of invoices electronically. Health data is considered sensitive data within the meaning of the Federal Act on Data Protection (FADP), meaning that special measures need to be taken when processing such data. Therefore, service providers who wish to send copies of their invoices



electronically are responsible for ensuring secure communication by taking appropriate technical and organisational measures

in accordance with Article 7 FADP and Article 8ff. of the Ordinance to the Federal Act on Data Protection (OFADP) such as the use of encryption and multi-factor authentication. The obligation to implement appropriate security measures is also discussed in the following text. It outlines the plan envisaging that all invoices should be sent electronically in the future in the compulsory health insurance system.

Service providers who fail to implement appropriate data protection and security measures can face serious civil and criminal consequences. Data subjects who have suffered an unlawful breach of their privacy will be able to take action individually and initiate civil proceedings or claim damages and compensation for any moral damage they may have suffered, for example as a result of the malicious interception of unencrypted emails resulting in disclosure of their health data to third parties. Criminal proceedings may also be initiated in the event of a breach of patient confidentiality, for example in the case of disclosure of medical information to unintended recipients.

Furthermore, service providers who choose to send copies of their invoices electronically must inform policyholders in advance of the risks associated with this method of transmission. Service providers are also required to ensure that the data subjects have freely and expressly consented to receiving copies of the invoices electronically. If a patient refuses to receive copies of invoices electronically, the service provider must respect their choice and send them hard copies instead by post at no extra cost to the patient. Finally, the law also provides that the insurance company and the service provider may agree that copies of invoices be sent to the patient by the insurance company.

ELECTRONIC INVOICING

Project regarding the transmission of electronic invoices in compulsory health insurance

In an effort to contain healthcare costs, the Federal Council has adopted a range of measures including the requirement for all healthcare providers in inpatient and outpatient settings to send their invoices electronically. The FDPIC intervened in the consultation procedure to clarify the data protection and security requirements.

On 7 September 2022, the Federal Council adopted the dispatch on a draft amendment to the Federal Health Insurance Act (KVG/LAMal) relating to the second package of measures to control healthcare costs. The package includes an amendment to Article 42 paragraph 3ter of the Federal Health Insurance Act which provides that in future all providers of inpatient and outpatient services will be obliged to

send their invoices electronically regardless of whether these are to be paid by the health insurance company (third-party payer) or by the policyholder (third-party guarantor). In the third-party paver system, the policyholder is sent an electronic copy - or, if they prefer, a hard copy, free of charge – of the medical invoice that was sent to the insurance company for them to check; In the third-party guarantor system, the policyholder is sent an electronic invoice - or, if they prefer, a hard copy, free of charge - for them to check and pay. The policyholder then emails the invoice to the health insurance company or validates it on the insurer's online portal. In the case of a paper invoice, the policyholder sends it to the insurance company, which then asks the service provider to send them an electronic copy. The exact procedure will be set out in an ordinance.

The details regarding the electronic transmission of invoices will be defined by the tariff partners. Service providers and insurance companies or their associations will need to reach an agreement on a single national standard. The plan is for invoicing to be carried out on a platform via a standardised form designed to ensure data

security. If the parties fail to agree on a single system within a two-year transition period, the standard will be set by the Federal Council.

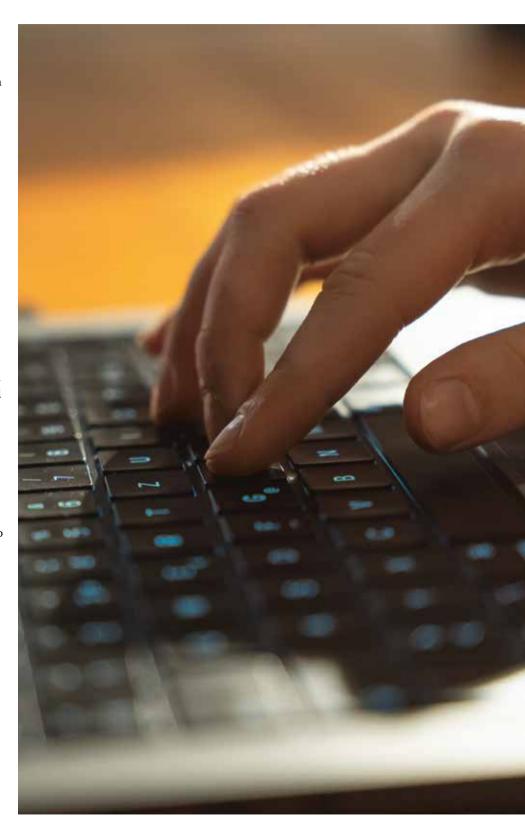
During the office consultation procedure, the FDPIC noted that the version of the draft dispatch submitted for consultation needed to be clarified regarding the technical and organisational measures to be implemented. The FDPIC also reiterated that the entry into force on 1 January 2022 of the new Article 42 paragraph 3 of the Federal Health Insurance Act regarding the electronic transmission of invoice copies to policyholders had clearly highlighted the risks inherent in the use of electronic versus paper invoices and the need for service providers to implement appropriate technical and organisational measures such as encryption and multi-factor authentication. The obligation to implement appropriate security measures is also discussed in the preceding text, which outlines the current obligation to send copies of medical invoices.

Following our proposals, the draft dispatch was modified, and the section on data protection was amended to include a reference to the FADP standards, specifically the obligation to implement appropriate technical and organisational measures against unauthorised processing. It was also pointed out that invoices contain sensitive data within the meaning of the FADP as service providers are required to include in their invoices all the administrative and medical information needed in order to check the calculation of the invoice amount, in particular diagnoses and details of services provided. The dispatch specifies that the processing of such sensitive data requires the implementation of special measures (encrypted transmission and multi-factor authentication), which the tariff partners will need to take into account when developing a single national standard capable of ensuring data security. Finally, the dispatch was amended to specify that, when devel-



oping a single standard, the tariff partners will also need to take into account their obligations under the revised FADP: in par-

ticular, the project will need to undergo an impact assessment regarding the protection of personal data within the meaning of Article 22 of the revised FADP.



30th Annual Report 2022/23



1.5 Employment

FEDERAL EMPLOYEES

Retention of staff records by the FSO

The FDPIC opened a case investigation against the Federal Statistical Office (FSO) regarding the retention of physical federal staff records beyond the statutory retention period of ten years. After establishing that corrective action had been taken, he closed the investigation without any recommendations. In our previous Annual Report 2021/ 2022, the FDPIC stated that he had sought clarification from the Federal Statistical Office (FSO) regarding management of the physical records of former employees. The FDPIC had learnt that the FSO was keeping a large number of staff records beyond the statutory retention period of ten years. When contacted by the FDPIC, the SFO recognised the need for action and presented him with an implementation plan and timetable for restoring compliance with the law. The necessary work was to be completed by summer 2022. In light of the fact that the necessary action had not yet been taken by that time and given the delay

in planning, the FDPIC was forced to launch a formal investigation in a supervisory capacity under Article 27 FADP to ensure that the FSO take measures promptly to rectify the legal situation and notify the FDPIC of the measures taken in that regard.

In November 2022, the FSO informed the FDPIC that the mandate for restoring the legal situation had been completed and that the old staff records had been sent to the Federal Archives, which had confirmed receipt. Non-archival records (including that of the person who had reported the case to the Commissioner) had been deleted, and the deletion log had been sent to the Federal Archives. The latter have

already clarified and agreed on the procedure to be followed for staff files dating between 2012 and 2017 (eDossiers from 2018).

Thus, the FDPIC received confirmation that the physical records of archival value had been sent to the Federal Archives, whereas the others had been destroyed. As a result, he has established that the FSO currently no



longer retains records beyond the statutory retention period, and clear filing procedures are now in place to comply with

the legal requirements for filing and destruction of future records that are currently less than ten years old.

Therefore, the FDPIC was able to close the investigation in January 2023 without any recommendations as the FSO had taken the necessary corrective action to restore compliance with the legislation governing federal personnel and data protection.

30th Annual Report 2022/23

1.6 Traffic and transport

SWISS FEDERAL RAILWAYS

Passenger flow measurement at railway stations

In October 2022, Swiss Federal Railways (SBB) informed the FDPIC of a project aimed at measuring passenger flow at railway stations. As the project presents a high potential risk for passers-by, before implementing it, SBB will perform a data protection impact assessment (DPIA), which it will submit to the FDPIC for an opinion.

In February, the media reported on an SBB project involving the collection of data at railway stations for the purpose of optimising the flow of people. The text of the corresponding tender documents was initially misleading in places, resulting in accusations that SBB intended to monitor passengers

using facial recognition technology. SBB denied the accusations and as-



sured the public that the system used to measure passenger flow would work with anonymised data and that at no point

would the data be analysed in a nonanonymised form.

SBB's data protection officer had already informed the FDPIC about the project in October 2022. Although the sole purpose of the new passenger flow measurement system is to optimise the flow of people through railway

stations without identifying individuals, i. e. the data will be anonymised, the project is associated with a potentially high risk of (re)identification.

Therefore, SBB assured the FDPIC that, before implementing the project, it would carry out a data protection impact assessment, which it would submit to the FDPIC.

The SBB is confident that the project $\,$



can be implemented in a privacy-compliant manner. At the end of the reporting period, the FDPIC had no reason to believe

the contrary. The FDPIC will comment on the project after receiving the DPIA.



1.7 International

This past reporting year, with the pandemic easing, a number of international conferences could be attended again in person. Therefore, the FDPIC took the opportunity to attend a number of international events in person, specifically the meetings of the Council of Europe, the European Data Protection Commissioners' Conference and the Francophone Association of Data Protection Authorities.

The past reporting year has once again illustrated the international dimension of data protection. Companies that operate internationally face sensitive legal issues when transferring personal data across borders through data storage in clouds and on servers abroad, for which there is currently no case law in Switzerland (see Section 1.1). Against this backdrop, the FDPIC is following with great interest the EU's current efforts to issue a new adequacy decision for the US.

EUROPE

Council of Europe

After Russia's withdrawal from the Council of Europe, the Consultative Committee had to decide on the conditions of its participation. As a result, the plenary session was postponed from June to November. The Consultative Committee also adopted guidelines on digital identity. It then elected the representative of Switzerland as its first vice-chair.

The meetings of the Consultative Committee on Convention 108 and its Bureau could once again be held in person. Convention 108 is a treaty open for signature by non-member states of the Council of Europe. Russia's extraordinary withdrawal from the Council of Europe raises the question of the conditions of Russia's continued participation in all pending treaties. The plenary session was postponed from June to November pending input from the Committee of Ministers and a discussion of the matter with other committees concerned. As a result, only one plenary session could be held in 2022 instead of the usual two, which led to delays in the handling of various matters.

At the plenary session in November, the first issue addressed by the Committee was that of the conditions

of Russia's participation on the Committee. The legal framework provided that after a Member State left the Council of Europe in extraordinary circumstances, it would continue to be a contracting party to Convention 108 but its participation could be restricted or suspended in accordance with the rules of procedure. Against this backdrop, the Committee adapted its rules of procedure and restricted Russia's participation to general discussions on the interpretation of Convention 108. In addition, it stated that Russia could neither chair the Committee nor be a member of its Bureau.

The Committee also discussed drafts on the sharing of data between States for the purpose of combating money laundering and the financing of EUROPE

terrorism and for tax purposes as well as standard contractual clauses for cross-border transfers of personal data. The FDPIC representative is the rapporteur for standard contractual clauses.

The Committee then instructed a working group to develop an interpretative guide on the exceptions and restrictions to the scope of application of the modernised Convention 108 (Convention 108+).

At its plenary session, the Committee adopted guidelines on digital national identity. These published guidelines describe how the data protection principles of Convention 108+ are to be interpreted in this context and contain a number of recommendations for legislative bodies, data controllers, equipment manufacturers, service providers, and data protection authorities.

Finally, elections were held during the plenary session to renew the members of the Bureau of the Consultative Committee. The FDPIC representative, who had been a member of the Bureau until then, was elected first vice-chair. The Committee is now chaired by the German representative, and the Senegalese representative remains the second vice-chair.

European Data Protection Commissioners' Conference in Dubrovnik

At the European Data Protection Commissioners' Conference, discussions focused on the latest developments in cross-border disclosure of data and cooperation between data protection authorities in this area. Member authorities adopted a resolution on the need for prompt ratification of Convention 108+.

After a two-year break due to the pandemic, the 30th European Conference of Data Protection Commissioners was held in Dubrovnik on 19–20 May 2022 at the invitation of the Croatian data protection authority. Discussions focused on the latest developments and pending issues regarding cross-border disclosure of data. Practical

examples were used to discuss cooperation between data protection authorities and the awareness-raising of privacy concerns.

The Conference stressed the need to accelerate the ratification of Convention 108+, the modernised version of Convention 108, as the only legally binding international treaty on the protection of personal data. A resolution was adopted calling upon the governments of Council of Europe Member States, the governments of third countries party to the Council of Europe, the European Union and international organisations to accelerate the signing and ratification of Convention 108+. The authorities adopted a second resolution aimed at ensuring that the Conference was able to continue to deliver on its vision and mission regarding all priority issues shared by European data protection authorities. The FDPIC participated in a working group that focused on the future of the Conference and that proposed the aforementioned resolution.

30th Annual Report 2022/23 51

EUROPE

INTERNATIONAL

European Case Handling Workshop

This year's workshop focused on data protection authorities' handling of complaints, which have risen sharply since the GDPR came into force.

The Personal Data Protection Service of Georgia (PDPS) hosted the European Case Handling Workshop, a working group on data protection case handling, in Tbilisi on 17–19 November 2022.

More than 50 delegates of personal data protection authorities from 26 European and non-European countries attended the meeting. The European Data Protection Supervisor and the Data Protection Office of the International Committee of the Red Cross were also represented.

The FDPIC will host the next workshop, which will take place in Bern in November 2023.

Global Privacy Assembly

The 44th Global Privacy Assembly (GPA) adopted two resolutions at its annual meeting of 25–28 October. The participants decided to strengthen international cooperation in the fight against cyber crime and to set out principles for the appropriate use of facial recognition technology.

The FDPIC attended the 44th Global Privacy Assembly (GPA) conference online on the theme of 'A matter of balance: privacy in the era of rapid technological advancement'. The conference highlighted the importance of striking a balance between privacy and technologies that are based on personal data processing.

The conference's open session was largely devoted to the issues of privacy and human rights, with panels addressing surveillance in commercial settings and data protection challenges in humanitarian crises, as well as discussions on data protection and competition. It also included more traditional panels on a number of topical issues such as artificial intelligence, children's privacy and cross-border data transfer.

At the closed session, participants –including the FDPIC –agreed to work towards strengthening capacity for international cooperation on cyber security and defining principles for the appropriate use of facial recognition technology. In this forum, the FDPIC also spearheaded work on the role of personal data protection in international development assistance, international humanitarian aid and crisis management. The GPA adopted two resolutions:

 One aimed at improving cyber security regulation and understanding the harm caused by cyber incidents.
 This resolution explores opportunities for international cooperation **HUMANITARIAN AID**

and knowledge and information sharing, including technical expertise and best practices, amongst GPA members to facilitate investigations and regulatory activities relating to cyber security issues. A dedicated working group will deliver exploratory work on this topic by autumn 2023;

 The other resolution concerns facial recognition. This resolution outlines six key principles and expectations for organisations using facial recognition technology.

The FDPIC actively contributed to this work and co-authored both resolutions. Finally, Jersey's information commissioner, Paul Vane, was selected to serve as a member of the Executive Committee.

GPA working group

The protection of personal data is crucial to humanitarian aid. The GPA's dedicated working group WG AID has carried out various activities aimed at advancing privacy protection in emergency situations.

In a humanitarian crisis such as armed conflict or natural disaster, the rule of law is not always fully observed.

Therefore, two years after it was set up, the Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management (WG AID) has strengthened its activities.

During the year under review, it focused its energy on updating its 2021–2022 work plan in line with the GPA's strategic priorities, specifically those relating to the advancement of privacy protection worldwide. To this end, it distributed a questionnaire, updated its mapping of relevant actors and strengthened relations with other international bodies and networks that advance data protection and privacy issues.

In accordance with the objectives set out in the resolution, members of the WG AID pursued the following general goals:

- To respond to requests for cooperation from relevant parties to develop guidelines and share best practices in privacy and data protection taking into account the specificities of international development aid and international humanitarian aid as well as the need to facilitate these activities:
- To develop an advocacy and engagement strategy with relevant stakeholders.

In order to achieve these two goals, the WG AID engaged in the following activities in particular:

 Establish sustained contact with the relevant actors at both bilateral and multilateral levels and thus maximise the reach of the GPA's voice by strengthening relations with the actors of international development aid;

30th Annual Report 2022/23 53

AFAPDP

- In collaboration with other relevant working groups of the GPA, look into producing documents and advocacy tools for better consideration of data protection and privacy in relevant activities;
- Promote and facilitate, for the recipient countries benefiting from these activities that do not have legislation on data protection and privacy, their integration into the global data protection and privacy community.

This included various activities such as regularly updating the mapping of international development aid and international humanitarian aid as well as identifying the recipient countries benefiting from these activities that do not have legislation on data protection and privacy.

The WG AID was established in 2020 during the 42nd Global Privacy Assembly (GPA). On that occasion, the FDPIC presented a resolution on the role of personal data protection in international development aid, international humanitarian aid and crisis management. Since then, he has chaired the working group on this issue, which currently has more than 20 members.

Francophone Association of Data Protection Authorities

The members of the Francophone Association of Data Protection Authorities (AFAPDP), including the FDPIC, met in Tunis on 3–4 October 2022 for the two-day conference entitled 'Rencontres francophones de la protection des données personnelles'.

The conference was attended by independent authorities from 23 countries sharing a common language, values and legal tradition. This year's work focused on the concept of identity in all its forms – sovereign and digital – as well as on issues related to cooperation and the role of personal data protection in international aid, with discussions moderated by the FDPIC. In her

capacity as Secretary General of the AFAPDP, the chair of the French data protection authority CNIL, Marie-Laure Denis, called on the independent data protection authorities to work together to make their voices heard in the implementation of the 2022–2026 Digital Francophonie Strategy with particular regard to the enhancement of data protection and regulation of the data economy.

The AFAPDP also held its Annual General Meeting, during which members adopted the Tunis declaration on the protection of personal data. The declaration underlines the importance of protecting personal data, stressing that data protection is a precondition for the exercise of other rights and freedoms of individuals and, in that sense, constitutes a fundamental right in our democratic societies. The members also elected the new Bureau, of which the FDPIC is a member.



BILATERALLY

INTERNATIONAL COOPERATION

SCHENGEN

Visit by a Tunisian delegation

As part of the TRUST programme for an accountable transition for Tunisia, Switzerland intends to draw on its experience to improve the governance of Tunisia's public services by strengthening accountability, thereby increasing trust between citizens and institutions.

Under this programme, the FDPIC, Mr. Adrian Lobsiger, welcomed his Tunisian counterparts in Bern on 11 May 2022, namely Mr. Chawki Gaddès, head of the Tunisian data protection authority (INPDP), and Mr. Adnène El Assoued, president of the National Authority for Access to Information (INAI).

Their discussions focused on the different legislative frameworks and the issues linked to the increasing digitalisation of society. International cooperation plays a key role in the FDPIC's activities, and this meeting underlines just how important it is. The meeting provided an opportunity to highlight the importance and universal nature of data protection in our democratic societies as a fundamental right and a precondition for the exercise of other fundamental rights.

Privacy Symposium in Venice

The first Privacy Symposium was held in Venice on 5–7 April 2022 and was attended by more than 170 participants, including the FDPIC. The event aims to promote international dialogue, cooperation and knowledge sharing on data protection regulations, compliance and emerging technologies.

Covering topics ranging from health data protection to artificial intelligence and quantum computing as well as other topics relevant to the present and future of privacy, the conference demonstrated just how important it was to bring together legal experts, practitioners and the research community. It highlighted the potential of joining forces to support and enhance data protection across borders and technologies.

A representative of the FDPIC presented the new Federal Act on Data Protection, the latest developments in certification in Switzerland and the role of data protection in humanitarian action.

Border Travel and Law Enforcement Group

With the Commissioner present, the Border Travel and Law Enforcement (BTLE) group of the European Data Protection Board (EDPB) discussed issues relating to the Schengen acquis such as the use of facial recognition in law enforcement and the 2022 European Court of Justice ruling on Passenger Name Record data.

The FDPIC attended the meetings of the Border Travel and Law Enforcement group, an expert subgroup of the European Data Protection Board, to discuss Schengen-related issues.

The group discussed a code of practice for law enforcement agencies, namely the Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement, which it adopted in May 2022.

The group also discussed the ruling of 21 June 2022 by the Court of Justice of the European Union (CJEU) on implementation of the Passenger Name Record (PNR) Directive. The Directive regulates the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The CJEU has set out strict limitations to be observed by

SCHENGEN

Member States during implementation of the PNR Directive. For example, it limits the purposes set out in the PNR Directive, which are exhaustive. The PNR system should be used only in connection with terrorist offences and serious crime and not for ordinary crime. There should be no indiscriminate application of the general retention period of five years to all air passengers' personal data.

Following the preliminary work by the BTLE, the EDPB adopted the Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of Directive (EU) 2016/681 on the use of PNR data in Member States on 13 December 2022. Even though Switzerland is not bound by CJEU rulings, this should be taken into account in the current legislative process for a new Passenger Name Records Act (PNRA).

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

The SIS Supervision Coordination Group focused on the new evaluation and monitoring mechanism and the new SIS legal framework.

The SIS II, VIS and Eurodac Supervision Coordination Groups are bodies set up under EU law to monitor the protection of personal data in the corresponding information systems. They are composed of the European Data Protection Supervisor and representatives of the national data protection authorities.

With the introduction of the new evaluation and monitoring mechanism, Schengen Member States, including Switzerland, will in future be evaluated every seven years instead of every five. A pool of experts will also be created. For the Schengen data protection evaluations, the FDPIC has appointed an expert who has already been nominated for an evaluation.

Furthermore, under the new SIS legal framework, the European Data Protection Supervisor and the national supervisory authorities – including the FDPIC – will meet at least twice a year within the framework of the European Data Protection Board (EDPB). The biennial activity report of the SIS II SCG was adopted.

As has been common practice for years now in other areas of Schengen evaluation, aspiring data protection experts should now also be offered training. Furthermore, in the future, persons seeking to join the pool of experts will no longer be required to undergo security clearance.

SCHENGEN

SCHENGEN

Schengen Coordination Group of the Swiss data protection authorities

The federal and cantonal data protection authorities and those of the Principality of Liechtenstein exchanged information within the framework of the Schengen Coordination Group chaired by the FDPIC.

The FDPIC provided an update on the work carried out by the European SIS II and VIS Supervision Coordination Groups that had met in Brussels on 1–2 June and 22–23 November 2022, while the cantonal data protection authorities reported on their experiences with inspections.

A sub-working group composed of representatives of the FDPIC and of the cantons of Basel-Land and Zurich updated the guidelines on monitoring of the use of the Schengen Information System to bring them in line with the new European legal situation. These serve mainly as guidance for the cantonal supervisory authorities when carrying out inspections. Furthermore, the representatives reported on their experiences and findings from their official inspections, specifically of log files. In the future, their experiences will be collected in a structured way.

Schengen-related activities at the national level

The EU postpones its evaluation of Switzerland by two years to 2025.

The Schengen evaluation of Switzerland that the EU had originally scheduled for early 2023 has been postponed by two years. This decision comes after the adoption of Council Regulation (EU) 2022/922 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis, which will apply in the EU area from February 2023. As a development of the Schengen acquis, this regulation will only be applicable in Switzerland at a later date as it first needs to be approved by the Federal Assembly and then implemented in national legislation. This delay in the application of the regulation also means that the EU

Commission will now be evaluating Switzerland in 2025 instead of 2023 as originally planned.

In addition, the EU Commission has called on Schengen States to appoint data protection experts to evaluate other states. To this end, the Federal Office of Justice and the FDFA organised a Schengen evaluation (SCHEVAL) meeting of experts on 12 May 2022. Experts from various areas such as police cooperation, SIS/SIRENE and data protection informed those present, including future experts, about cooperation with the European Commission, the evaluation process and training opportunities, and gave practical advice.

In the year under review, the FDPIC also initiated an audit at fedpol as the central access point to C-VIS (Central Visa Information System) data on its retrieval of said data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. He began by sending out a questionnaire and obtained answers to further questions during an on-site visit. Once he has established the facts, the FDPIC will carry out a legal analysis.



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 public 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 first half of the 2022 reporting year was marked by the lingering effects of Covid-19 as we approached the tail end of the pandemic. The figures provided by the Federal Administration regarding the number of requests received in 2022 for access to official documents indicate that the media and society's need for specific, transparent information is as strong as ever.

Although the federal authorities received slightly fewer applications for access during the year under review compared with the previous year, the figure remains high.

Many of the applications for access required significant resources to process, not least because they were often extensive and necessitated coordination with other offices and departments. 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 129 mediation requests during the year under review, namely 13% fewer than the previous year. The purpose of mediation is to enable a swift agreement between the parties. The measures introduced for this purpose with the pilot project

in 2017, and, in particular, the primacy of the oral mediation procedure, proved successful again in 2022. 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 74% of cases.

In January 2022, with the pandemic still under way and people still obliged to work from home, the FDPIC had to suspend face-to-face mediation sessions as these could not be held by video conference for data protection reasons among other things. In the 11 mediation procedures for which an oral mediation session could not be held because of the pandemic and which had to be conducted by correspondence instead, no settlement was reached.

The lower proportion of amicable outcomes and the larger number of mediation procedures that had to be carried out by correspondence due to the pandemic resulted in longer processing time, creating a backlog in the completion of procedures. The figures clearly underline just how important face-to-face on-site mediation sessions are for the swift conclusion of mediation procedures.

The pandemic, the consistently large number of mediation requests received and the increasingly complex legal issues mean that the FDPIC is exceeding the statutory processing time of 30 days in an increasing number of cases. The FDPIC believes that the additional resources allocated by Parliament will help him to reduce processing time again (see Section 2.3 for more details).

This reporting year saw further efforts to exclude more areas of the Administration's activities and certain categories of documents from the Freedom of Information Act (e.g. "rescue umbrella" for the electricity industry, see Section 2.4). Restricting the

scope of the Freedom of Information Act in this way undermines the principle of freedom of information and the transparency within the Administration that it seeks to achieve. The FDPIC now publishes an up-to-date overview of special reservations under Art. 4 FoIA in the Annual Report (see Section 2.5).

The FDPIC notes that most parts of the Administration have embraced and are actively implementing the paradigm shift brought about by the Freedom of Information Act. The federal authorities that are subject to the Freedom of Information Act have no direct influence on the number or scope of applications for access or the resources used to process them. During the year under review, we observed a trend towards an increase in the number of applications for access to transcripts of electronic communications.

However, the Administration and its freedom of information advisors are responsible for ensuring the consistent application of the provisions of the Freedom of Information Act and the relevant case law. The FDPIC has observed that some parts of the Federal Administration do not make sufficient use of the possibilities provided by the Freedom of Information Act to protect their confidentiality interests and, for example, fail to apply access restrictions with the level of justification required by case law. In this context, the FDPIC refers to his written recommendations, which are published in their entirety on his website (www.derbeauftragte.ch). These show that during the year under review, in a few cases, the Administration refused to comply with the Freedom of Information Act. In individual cases, for example, it denied the FDPIC access (required by law without exception) to documents that were the subject of a mediation request that had been filed, preventing the FDPIC from carrying out his mediation activities.

30th Annual Report 2022/23 **63**

2.2 Applications for access slightly down in 2022

According to the figures released, the federal authorities received 1153 applications for access to information in the year under review, i.e. 15% fewer than in 2021 (1385). In 2022, the authorities also processed 27 applications for access that had been submitted in previous years. They granted full access in 624 cases (53%), compared with 694 (50%) in 2021. In 236 cases (20%), access to the documents applied for was partially granted or deferred, compared with 324 (23%) the year before. In 99 cases (8%), access was fully denied, compared with 126 cases (9%) in 2021. According to the authorities, 53 applications for access were withdrawn (5%) (compared with 48 (3%) in 2021), 69 applications were still pending at the end of 2022, and in 99 cases there was no official document.

The number of applications for access is likely to remain high in the coming years, even though the need for information and transparency, which had been particularly strong during the Covid-19 pandemic, decreased in the year under review. The authorities

have compiled statistics on applications for access to Covid-19 documents. which they have sent to the FDPIC along with the annual reporting data (see statistics on applications for access to Covid-19 documents highlighted in yellow). According to the federal authorities, 93 out of 1180 applications for access processed (8%) were for documents relating to Covid-19, considerably fewer than the previous year (24%). Full access was granted in 29 cases (31%), i.e. less frequently compared with the overall statistics. The authorities granted partial access or deferred access to Covid-19 documents in 35 cases (38%) – more frequently than for other documents - while access was fully denied in four cases (4% or half the overall percentage). Seven applications for access were withdrawn, eight were still pending at the end of 2022, and in ten cases there was no official document. Society is likely to continue to review the government measures introduced to combat the pandemic, meaning that further applications for access and mediation requests relating to the pandemic can be expected in 2023.

In summary, the FDPIC notes that, since 2015, full access has been granted to the requested documents in at least 50 % of cases, while the number of applications for access which have been fully denied has stabilised over the years at just under 10 %.

Federal departments and federal offices

Several administrative units were the focus of much media and public attention in 2022. As in the previous pandemic years, due to the nature of their work, the FDHA (198), the DDPS (294) and the FDFA (164), in particular, received a large number of applications for access. In the case of the FDHA, 38% of the applications for access received by all offices concerned official Covid-19 documents, compared with 63% the previous year. The authorities in question reported that the applications received were sometimes very

extensive and complex, many requiring time-consuming coordination between federal offices or departments.

The figures released by the federal offices indicate that the FOSPO received the most applications for access in 2022, namely 220. The FOPH reported receiving 91 applications in the year under review, 57 of which were for access to Covid-related documents, followed by the FOEN with 61, and swissmedic and SECO with 37 each.

■ Total requests

Access granted

Seventeen authorities reported receiving no applications for access during the year under review. The FDPIC himself received 15 applications for access and granted full access in nine cases; he refused access altogether in two cases. One request was withdrawn, and three were still pending at the end of 2022. In 2022, fees charged for access to official documents totalled CHF 24 582.05, 65% more than the previous year (CHF 14 924.90). While the FDFA, the

FDF, the DDPS, the Parliamentary Services, the Office of the Attorney General of Switzerland and the Federal Chancellery charged no fees, the other four departments did invoice applicants for some of the time spent dealing with their applications (FDHA: CHF 19 646.50; EAER: CHF 4185.55; DETEC: CHF 500; FDJP: CHF 250). It should be noted that just 29 out of 1180 applications for access incurred a fee. Therefore, as in previous years,

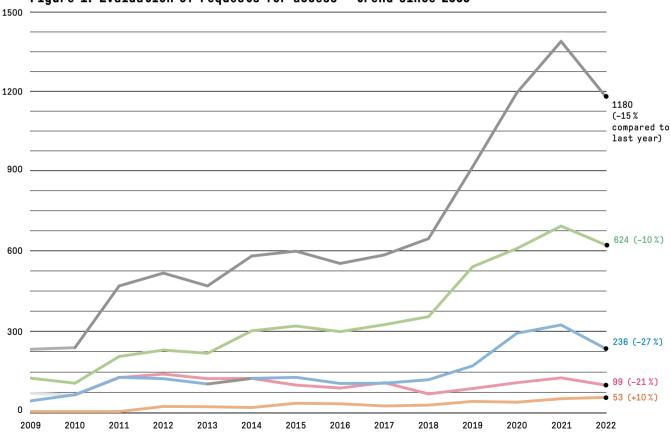


Figure 1: Evaluation of requests for access - trend since 2009

30th Annual Report 2022/23

Access partially granted or suspended

Access denied

pending



fee-charging remains the exception, with access being granted free of charge in just under 98% of cases.

The administrative practice, observed again in the year under review, of granting free access to official documents as a rule will be enshrined in the Freedom of Information Act. On 30 September 2022, Parliament adopted the principle of free access to official documents. By way of exception, the authorities may continue to charge fees after the entry into force of the amendment to the Act (yet to be decided by the Federal Council) if an application for access requires disproportionate effort to process. Therefore, the revised version of the Freedom of Information Ordinance will need to specify the number of working hours above which a fee may be charged for processing applications for access.

With regard to processing time for applications for access, the FDPIC points out that the authorities are under no obligation to record this and that there are no guidelines establishing 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 requests. According to the data received, the time

spent this reporting year amounted to 5,404 hours, slightly down from the year before (5,562 hours).

The fact that the amount of time reported by the authorities for processing applications for access does not reflect the full amount of time spent is illustrated, for example, by the data provided by the FOPH, which received a particularly large number of applications for access in connection with the pandemic. In addition to the 443 working hours reported by the FOPH's specialist units and the legal support provided by its freedom of information advisor amounting to 40 % full-time equivalents (FTEs), the FOPH again reported a large amount of time

(amounting to at least 3.5 FTEs) spent processing applications for access in connection with Covid-19 (including mediation requests and appeal procedures).

The time spent preparing mediation procedures also increased, totalling 1006 hours, compared with 865 hours in 2021, 569 in 2020, 473 hours in 2019, 672 hours in 2018 and 914 hours in 2017.

Parliamentary services

The Parliamentary services reported receiving no information requests during the year under review.

Office of the Attorney General of Switzerland

The Office of the Attorney General of Switzerland reported receiving six applications for access. It granted full access in five cases and refused access altogether in one case.

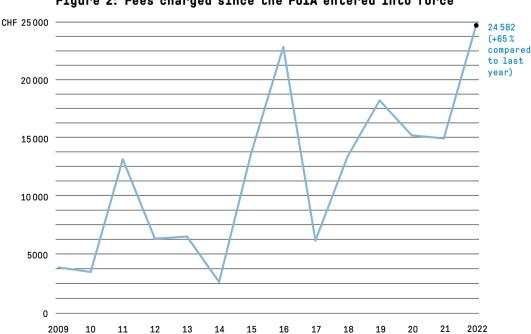


Figure 2: Fees charged since the FoIA entered into force

30th Annual Report 2022/23

2.3 Mediation procedures: mediation requests slightly down

In 2022, the FDPIC received 129 mediation requests, 13% fewer than in 2021 (149 requests). The majority of mediation requests was filed by journalists (47) and private individuals (37). Therefore, of the 434 cases in which the Federal Administration fully or partially refused access, deferred access or stated that there were no official documents, 129 cases (30%) resulted in a mediation request being filed with the FDPIC. Thirteen of these (9%) concerned official Covid-related documents.

In 2022, 115 mediation requests were settled, 93 of which had been filed during the reporting year and 22 the previous year. In 50 cases, the participants were able to reach a mutually acceptable agreement. The FDPIC also issued 31 recommendations, which

settled 48 cases which were unlikely to result in an agreement between the parties.

The cases dealt with include 13 mediation requests which had not been filed on time, three cases which did not satisfy the conditions for application of the Freedom of Information Act, and one request for mediation that was withdrawn.

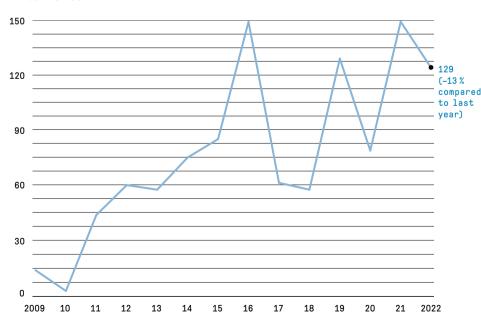
At the end of the year, 13 mediation procedures had been suspended by agreement between the participants or at their request.

Proportion of amicable outcomes

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

The ratio of amicable outcomes to recommendations is the best measure of the effectiveness of the measures introduced in 2017 and of oral mediation sessions. During the year under review, 50 amicable outcomes were achieved, and the FDPIC issued 31 written recommendations to settle 48 cases. Therefore, amicable outcomes were reached in 51% of cases.





However, this needs to be explained: amicable solutions are typically only reached when mediation sessions take place. In the 43 mediation sessions that took place during the year under review, an agreement was reached in 32 cases (75%). As mentioned in Section 2.1, face-to-face mediation sessions with the parties had to be suspended between 20 December 20211 and 3 February 20222 because of the measures introduced to stop the spread of Covid-19, and so in 11 mediation requests a session had to be waived. No agreement was reached in any of the procedures conducted by correspondence during that time, which affected the statistics accordingly.

In conclusion, oral mediation sessions are crucial in order to achieve the objectives set out in legislation and

beneficial for all parties involved in the mediation procedure. The FDPIC will continue to favour and promote face-to-face mediation over mediation by correspondence.

Table 1: Amicable outcomes

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 re-examine 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 procedures are extended.

The table shows that just 25% of mediation procedures completed in 2022 were concluded within the 30-day period, while 42% took between 31 and 99 days, and 33% took 100 days or more.

30th Annual Report 2022/23 **69**

¹ Art. 20 of the Covid-19 Special Situation Ordinance; FCD of 17.12.2022.

² Art. 25 para. 5 of the Covid-19 Special Situation Ordinance; FCD of 2.2.2022; Measures and ordinances (admin.ch).

Furthermore, of the 29 mediation requests settled within the 30-day period, only 17 (59%) 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 12 cases (41%), no substantive assessment was made. These were mainly cases that clearly fell outside the scope of the Freedom of Information Act or cases in which the formal requirements for initiating mediation were not met.

As explained above, mediation procedures took longer again during the year under review because of the pandemic, increasing the processing backlog further. Moreover, the number of mediation requests received is typically subject to fluctuation. For example, the FDPIC received a large number

of requests in March (21) and August (27) but only three in June and none at all in November.

The statutory 30-day deadline for completing the mediation procedure was regularly met in previous years when the parties reached an agreement during the mediation sessions. This was not the case in the year under review: When during the mediation sessions an agreement was reached, the 30-day deadline was met in just 29 % of cases compared with 60% the previous year. When an amicable solution could not be reached and the FDPIC had to issue a written recommendation to the parties involved, only in three cases (6%) 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 applications for access, the large number of third parties involved in the procedure, or complex legal, technical or political issues. These explanations also apply to the 38 cases that took 100 days or longer to process. Delays

were further compounded by the large number of documents and persons concerned involved. In situations such as these involving a substantially heavier workload, the FDPIC may extend the deadline by an appropriate period in accordance with Article 12a of the Ordinance on Freedom of Information in the Administration (FoIO; SR 152.31).

The legislator has designed the mediation procedure as an informal and non-prejudicial procedure for amicable resolution of disputes. However, experience shows that the involvement of legal representatives by the applicants or by third parties being consulted at the access and mediation procedure stage is hardly conducive to a straightforward, pragmatic and swift solution.

Table 2: Processing time of mediation procedures

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

^{*}Source: Presentation by the Commissioner, event marking the $10^{ ext{th}}$ anniversary of the FoIA, 2 September 2016

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 2023, 41 mediation cases were still pending, including 13 suspended procedures (one from 2019, one from 2020, three from 2021, and eight from the year under review). 16 cases had been settled by the time this report had been completed.

Table 3: Pending mediation procedures

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

CYRERSECURITY

The amendment of the Information Security Act (ISA)

The FDF has opened a consultation procedure on the draft amendment of the Information Security Act to include a duty to report cyber attacks on critical infrastructure. This amendment involves restricting the principle of freedom of information.

In response to the growing number of cyber incidents involving private individuals, businesses and the authorities, the Federal Council has instructed the FDF to draw up a bill establishing the legal basis for introducing a duty to report cyber attacks on critical infrastructure. This reporting duty is intended to give the National Cyber Security Centre (NCSC) a better overview of cyber attacks in Switzerland, to help the victims to deal with the cyber attacks, and to warn other operators of critical infrastructure. In addition to the duty to report cyber incidents, the ISA shall also define the tasks of the NCSC and appoint the NCSC as a central reporting office for cyber attacks.1

The bill prepared by the FDF was submitted to the parties concerned for consultation. Following the consultation, a minority of participants (6 out of 102 according to the FDF) argued that reports submitted to the NCSC should be excluded from the Freedom of Information Act. This view was taken into account, and a special provision within the meaning of Art. 4 FoIA was added to Art. 4 para. 1bis ISA providing that information regarding third parties that comes to the attention of the NCSC through reports and in the course of analysing these may not be made accessible under the Freedom of Information Act.

Although the FDPIC understands the importance of reports and the need to process them for Switzerland's security, he has opposed the introduction of this new special provision as he considers it disproportionate. The provision in question undermines the principle of freedom of information by refusing the public access to information relating directly to the performance of a key duty of the NCSC and thus preventing the state control sought by the legislator in an area of great concern to the public. In particular, the FDPIC found that the wide range of exceptions (e.g. Art. 7 para. 1 let. c FoIA, which protects Switzerland's internal and external security, Art. 7 para. 1 let. g FoIA, which protects business secrets, and Art. 7 para. 2 FoIA, which protects privacy) provided for in the Freedom of Information Act was sufficient to protect the various interests in question. For these reasons, the FDPIC does not see how applying the Freedom of Information Act would hamper the FDF in its role as a central reporting office and has requested that the special provision be deleted.

The FDF has partly taken into account the FDPIC's views and has limited the scope of the exception.

¹ Consultation procedures completed – 2022 (admin.ch)

ELECTRICITY INDUSTRY

Art. 4 para. 1bis now states that information regarding third parties that comes to the attention of the National Cyber Security Centre (NCSC) in its work of receiving and analysing reports in accordance with Section 5 shall not be made accessible under the FoIA. specifying that the authorities, organisations and persons referred to in Article 2 para. 1 FoIA are not considered third parties. Despite this specification, which the FDPIC welcomes, the discrepancy has been maintained for the reasons already mentioned and appears in the dispatch as well as in the draft submitted to the Federal Council.

Preliminary draft of the Federal Act on a "rescue umbrella" for the electricity industry

Information provided by systemically critical companies in the electricity industry regarding the provision of financial aid is excluded from the right of access under the Freedom of Information Act. The FDPIC had unsuccessfully opposed this restriction of the freedom of information in the legislative process.

The so-called 'rescue umbrella' for the electricity industry is enshrined in the Federal Act on Subsidiary Financial Aid to Support Systemically Critical Companies in the Electricity Industry (FiRECA) and is intended to help guarantee the supply of electricity in Switzerland, specifically by regulating financial aid for systemically critical companies in the electricity industry. According to Article 20 paragraph 4 of the Act. access under the Freedom of Information Act to information and data provided by systemically critical companies is excluded. The dispatch explicitly describes this as a special provision within the meaning of Article 4 letter a FoIA.

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. Reservations of this sort undermine the principle of freedom of information and the transparency within the Administration that the principle seeks to achieve.

Having not been consulted by the Administration during the interdepartmental consultation, the FDPIC opposed the introduction of this special provision during the joint reporting procedure, pointing out the goals of the Freedom of Information Act, namely to promote transparency with

ARCHIVIING ACT

regard to the activities of the Administration and to prevent mismanagement in relation to the granting of state loans and subsidies to the detriment of taxpayers.

The DETEC justifies restricting the principle of freedom of information on the grounds that the information and data in question are sensitive and often contain business or manufacturing secrets within the meaning of the Freedom of Information Act. During the consultation procedure, the FDPIC pointed out, in vain, that justified private interests remained protected even when the Freedom of Information Act was applied. The Act explicitly guarantees the protection of business secrets (Art. 7 para. 1 let. g FoIA) and of the privacy and personal data of natural and legal persons (Art. 7 para. 2 FoIA, Art. 9 para. 2 FoIA and Art. 19 FADP). Finally, the FDPIC pointed out that denying the public access to documents, particularly with regard to such a sensitive matter as the granting of financial aid, as was the case with the Covid-19 Loan Guarantees Act (see 28th Annual Report, Section 2.4), undermined the very foundation of the Freedom of Information Act.

Revision of the Federal Act on Archiving needed

The Archiving Ordinance is to be 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. In the FDPIC's view, these aspects cannot be clarified in a legally binding manner with a partial revision of the Archiving Ordinance.

The Archiving Act (ArchA) and the Freedom of Information Act regulate two different procedures for access to official information, which differ in various key aspects. The Archiving Act, which came into force on 1 October

1999, provides for long retention periods, largely stemming from the principle of secrecy prevalent in the Federal Administration at the time. Just a few years later, the legislator embraced a paradigm shift towards the principle of freedom of information (passive information, i.e. access on request) without expressly stating how official documents were to be dealt with under the Freedom of Information Act after they had been archived. For that reason, there are no binding requirements for the substantive or formal coordination of the Archiving Act and the Freedom of Information Act. This creates considerable legal uncertainty for members of the public and the authorities applying the law when it comes to determining the applicability and scope of the Freedom of Information Act and the Archiving Act in relation to applications for access concerning archived official documents submitted under the Freedom of Information Act during the retention period.

An evaluation has been carried out on behalf of the Federal Archives: The final report identifies the need for action in nine priority areas and includes recommendations. With regard to coordination of the Archiving Act and the Freedom of Information Act, the report recommends, for example, that the legislator specifies which law applies to applications for access under the Freedom of Information Act regarding archived official documents during the retention period.

However, according to the Federal Archives, the recommendations in the report on evaluation of the ArchA, including coordination of the Archiving Act and the Freedom of Information Act, can be implemented through appropriate archiving practices and an amendment to the Archiving Ordinance by the Federal Council. Therefore, the Federal Archives do not deem it necessary for the legislator to revise the Archiving Act.

In the FDPIC's view, the main problems are the lack of a legal framework for coordination between the Archiving Act and the Freedom of Information Act and the corresponding procedures for access to official information, which differ significantly in some respects. The number of archived files containing official documents under the Freedom of Information Act will increase in the future, so we can also expect a significant increase in the number of applications for access. Without clarification as to how the laws are to be formally coordinated, the authorities applying the law and the FDPIC himself risk being accused of overruling the legislator's intent expressed in the Archiving Act (with

long retention periods) or the Freedom of Information Act (freedom of information within the Administration) when they apply or fail to apply either act in individual cases. As a result, in the interdepartmental consultation on the discussion document regarding the need to revise the Archiving Act, the FDPIC maintained that coordination of the Archiving Act and the Freedom of Information Act was crucial given the far-reaching consequences and that it needed to be regulated by the legislator. Therefore, he considers the envisaged level of regulation in the Federal Council's Ordinance insufficient for proper coordination.

30th Annual Report 2022/23

FINANCE

Entry into force of the Anti-Money Laundering Act and Anti-Money Laundering Ordinance

The supervisory activities of the Central Office for Precious Metals Control (ZEMK in German), delegated to it by FINMA, are excluded from the personal scope of application of the Freedom of Information Act. The FDPIC unsuccessfully opposed this further restriction of the principle of freedom of information.

The Swiss Federal Central Office for Precious Metals Control (ZEMK) is attached to the Federal Office for Customs and Border Security and is responsible for all activities involved in supervising the movement of precious metals and precious metal products. In this area, the revised Anti-Money Laundering Act adopted in 2021 gives the ZEMK the mandate as a money laundering oversight authority, previously the remit of the Swiss Financial Market Supervisory Authority (FINMA) and self-regulatory organisations (SROs).

As part of the revision of the Anti-Money Laundering Ordinance, the supervisory activities of the ZEMK regarding trade assayers dealing in bank precious metals have been excluded from the personal scope of application of the Freedom of Information Act in accordance with the provision of Article 2 paragraph 2 FoIA and Article 1a of the corresponding Freedom of Information Ordinance. The State Secretariat for International Finance (SIF), which is responsible for amending the Anti-Money Laundering Ordinance, has justified this on the grounds that the persons and entities now supervised by ZEMK should be subject to the same rules that applied when they were supervised by FINMA and SROs.

In Article 2 paragraph 2 FoIA, the legislator excludes the Swiss National Bank (SNB) and FINMA from the personal scope of application of the Freedom of Information Act. However, in the revised version of the Anti-Money Laundering Act, having regard to the principle of freedom of information, it has decided not to exclude the ZEMK or its supervisory activities – recently

taken over from FINMA – from the personal scope of application of the Freedom of Information Act. In so doing, the legislator has upheld the principle of transparency applicable within the Federal Administration with regard to the supervisory activities of the ZEMK. Therefore, in the FD-PIC's view, the legislator has no intention of restricting the personal scope of application of the Freedom of Information Act.

The FDPIC also pointed out to the SIF that the wording of Article 2 paragraph 2 FoIA was clear and unequivocally excluded (only) FINMA and the SNB from the personal scope of application of the Freedom of Information Act. Furthermore, no reference was made elsewhere to the possibility of amending this provision in the Freedom of Information Ordinance. In the FDPIC's view, Article 2 paragraph 2 does not provide an adequate or sufficient legal basis for excluding the supervisory activities of the ZEMK from the personal scope of application of the Freedom of Information Act by creating a provision to that effect in the ordinance.

TOBACCO CONTROL ACT

Partial revision of the Federal Act on Tobacco Products and Electronic Cigarette

In the third quarter of 2022, the Federal Council opened a consultation procedure on a partial revision of the Federal Act on Tobacco Products and Electronic Cigarettes, which, among other things, provides that company advertising expenditure declared to the FOPH will be excluded from the principle of freedom of information. The FDPIC has opposed this.

On 1 October 2021, the Parliament approved the new Federal Act on Tobacco Products and Electronic Cigarettes (LPTab in French). Following the adoption on 13 February 2022 of the people's initiative 'Yes to protecting children and young people from tobacco advertising (no tobacco advertising to children and young people)', the

FOPH laid down provisions aimed at introducing additional restrictions in the LPTab on advertising, promotion and sponsorship relating to tobacco products and electronic cigarettes. The preliminary draft seeks to exclude from the Freedom of Information Act all information disclosed to the FOPH by individual companies regarding their expenditure on advertising, promotion and sponsorship. This exclusion is motivated by the need to protect the private interests of companies and, more specifically, their business secrets.

During the interdepartmental consultation, the FDPIC opposed this exclusion, which he considered unnecessary as the Freedom of Information Act already contained an exception clause that protected 'professional, business or manufacturing secrets' (Art. 7 para. 1 let. g). In the FDPIC's view, companies' private interests are already sufficiently protected and taken into account by the Freedom of Information Act. Moreover, in the fight against smoking, there is strong interest in transparency, the main aim of the LPTab being to reduce smoking.

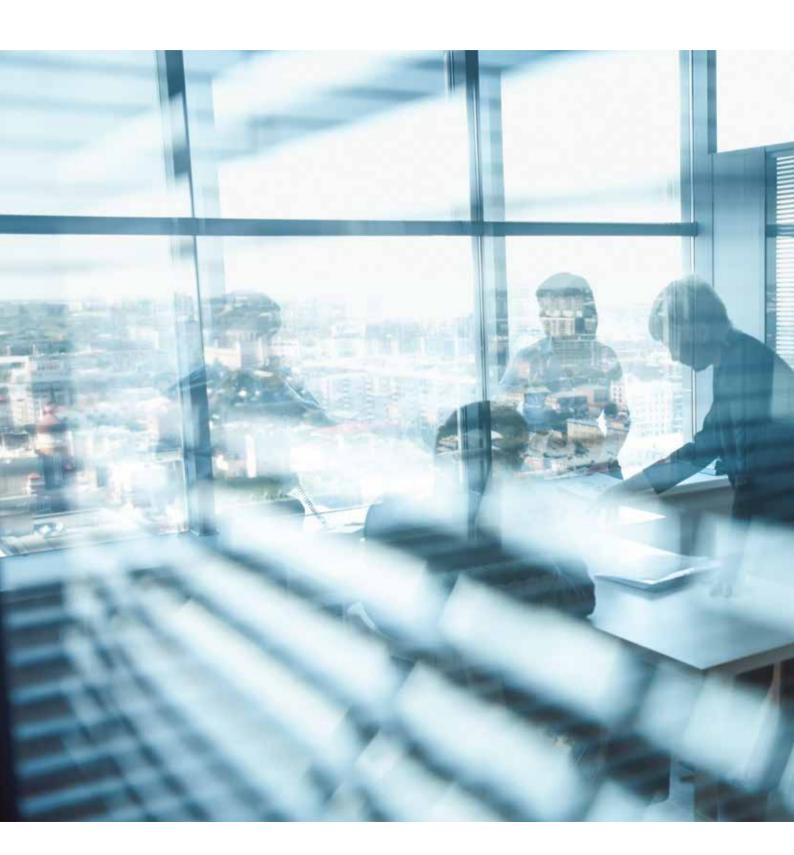
However, following the interdepartmental consultation, the FOPH informed the FDPIC about its decision to waive the exception to the principle of freedom of information. The dispatch on this issue is to be submitted to the Parliament in the first half of 2023.

ECONOMY

New Federal Act on the Screening of Foreign Investments (IPG in German)

The State Secretariat for Economic Affairs (SECO) conducted a consultation in the second quarter of 2022 on the introduction of the IPG. The original restriction of the principle of freedom of information has been deleted from the consultation draft.

In implementing the Rieder motion 18.3021, the Federal Council launched a consultation for the new IPG on 18 May 2022. The aim of screening foreign investments is to prevent any threat or danger to public order or security through takeovers of domestic companies by foreign investors. The SECO is to be responsible for implementing the screening of investments and for coordination with the other administrative units involved.





The SECO's original preliminary draft provided that the information provided and documents submitted to it in the course of its investment screening activities would not be publicly accessible. The intention was to exclude all information and documents from the scope of application of the Freedom of Information Act on the grounds that they were sensitive as they included business secrets or information provided by the Federal Intelligence Service (FIS).

In a preliminary consultation, the FDPIC opposed the introduction of this reservation, pointing out the significant public interest in the implementation of screening of foreign investments by the SECO. The business secrets of investors and information provided by the FIS are already protected by way of explicit exceptions regarding access provided for in the

Federal Act on Freedom of Information (Art. 7 para. 1 let. g FoIA and Art. 4 FoIA in conjunction with Art. 67 IntelSA). In addition, public interests affected in individual cases are already protected, in particular the execution of specific measures taken by an authority in conformity with its objectives (Art. 7 para. 1 let. b FoIA), the economic or monetary interests of Switzerland (Art. 7 para. 1 let. f FoIA), and free opinion-forming of authorities before decisions are made (Art. 8 para. 2 FoIA). The originally envisaged restriction of access has been deleted from the consultation draft.

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 provisions 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.

Table 4: Special provisions under Art. 4 FoIA

SR no.	Art./Para.	Entry into force:
832.10	Art. 52e HIA (preliminary draft)	Dispatch dated 7 September 2022 Status: not yet dealt with in Parliament
128	Art. 4 Abs. 1 bis	Planned as of 1 January 2024
952.3	Art. 6 para. 3	16 March 2023
734.91	Art. 20 para. 4	1 October 2022
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
951.26	Art. 12 para. 2	19 December 2020
742.101	Art. 14 para. 2	1 July 2020
743.01	Art. 24e	1 July 2020
745.1 747.201	Art. 52a Art. 15b	1 July 2020 1 July 2020
121	Art. 67	1 September 2017
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
420.1	Art. 13 para. 4 (see FAC ruling A-6160/2018 of 4 November 2019 E. 4)	1 January 2014
	832.10 128 952.3 734.91 172.056.1 951.26 742.101 743.01 745.1 747.201 121 817.0	832.10 Art. 52e HIA (preliminary draft) 128 Art. 4 Abs. 1 bis 952.3 Art. 6 para. 3 734.91 Art. 20 para. 4 172.056.1 Art. 48 para. 1 (explicit access provided); Art. 11 let. e (only considered a special provision during award procedures) 951.26 Art. 12 para. 2 742.101 Art. 14 para. 2 743.01 Art. 24e 745.1 Art. 52a 747.201 Art. 15b 121 Art. 67 817.0 Art. 24 Special provision in accordance with the dispatch on the Federal Act on Foodstuffs and Utility Articles of 25 May 2011 Art. 13 para. 4 (see FAC ruling A-6160/2018 of

Legislation (short form) and abbreviation	SR no.	Art./Para.	Entry into force:
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) Patents Ordinance (PatO)	232.14 232.141	Art. 90 Pat0 based on Art. 65 para. 2 PatA (see FSC ruling 4A_249/2021 of 10 June 2021)	1 July 2008
Entry into force of the Freedom of Information Act			1. July 2006
Parliament Act (ParlA)	171.10	Art. 47 para. 1 (see FAC ruling A-6108/2016 of 28 March 2018 E. 3.1)	1 December 2003
Goods Control Act (GCA)	946.202	Artt. 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	1 January 2010
Direct Taxation Harmonisation Act (DTHA)	642.14	Art. 39 para. 1	1 January 1993
		See ACLFA 2016.1 (pp.1-14), issued on 26 January 2016: Tax secrecy and access to official documents	
Federal Statistics Act (FStatA)	431.01		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:
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
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 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
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
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

(Non-exhaustive list)

The FDPIC



3.1 Duties and resources

Services and resources in the field of data protection

Number of staff

In its dispatch on the complete revision of the FADP, the Federal Council promised the FDPIC additional resources in the form of nine to ten staff positions (BBl 20177172). Switzerland's new Federal Act on Data Protection within the framework of the Application of the Schengen Acquis in Criminal Matters (SDPA, SR 235.3) already covers an aspect of the complete revision. The Federal Council implemented this Act on 1 March 2019 and promised the FDPIC three additional staff positions to handle his new duties and powers. This increased the headcount from 24 to 27 full-time equivalents (FTEs) in 2020. In spring 2021, in view of the entry into force of the revised FADP, originally scheduled for 2022, the FDPIC proposed that the Federal Council authorise the six remaining FTEs, which the Federal Council approved on 28 April 2021. This has increased the number of staff assigned to data protection by a further

five positions (one staff position was allocated to the Federal Chancellery for administrative services).

The Freedom of Information Act (FoIA) came into force in 2006. As the Federal Council never approved the three additional staff positions envisaged in the legislative dispatch, the FDPIC was forced to rely on his existing data protection staff and, in some cases, the Federal Chancellery's resources to fulfil his duties under the FoIA. After the Swiss Parliament which is now responsible for approving the FDPIC's budget - granted the FDPIC the staff positions envisaged in the legislative dispatch on 8 December 2022, the FDPIC was able to return one of these three positions to the Data Protection Directorate, thus increasing its headcount by one to a total of 33 staff positions. Given the increased workload in connection with mediation procedures, the FDPIC has assigned the two remaining positions to the Freedom of Information unit (see the following article entitled 'Services and resources in the field of freedom of information').

Given the extensive preparatory work required during the reporting period in preparation for the entry into force of the new FADP (new guidelines and texts for the website etc.), in terms of statistics, the newly recruited staff were deployed primarily in the information service group, as shown below.

Table 6: Staff positions available for FADP issues

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

30th Annual Report 2022/23

Table 7: Services in data protection

Table /: Services in da	ata prote	ction
Consultancy - Feder- al Administration	18,7%	
Consultancy - pri- vate individuals	21,1%	
Cooperation with foreign authorities	11,4%	
Cooperation with cantons	1,3%	
Total consultancy		52,5%
Supervision	14,7%	
Certification	0,0%	
Data collection register	0,4%	
Total supervision		15,1%
Information	20,2%	
Training, talks and presentations	2,0%	
Total information		22,2%
Legislation	10,2%	
Total legislation		10,2%
Total data protection		100,0%

Consultancy

As set out in the opening section entitled 'Current challenges', the FDPIC still faces a consistently high demand for consultancy services as he is required to support large digital projects. During the year under review, the proportion of staff working in consultancy amounted to around 52.5%. In the FDPIC's inspection plan for 2022, eight large projects are currently receiving support in the form of consultancy. Four of these projects are related to the digital transformation of the Federal Administration ordered by the Federal Council.

Over the course of the reporting period, three teams from the Data Protection Directorate responded to an average of 33 enquiries and complaints from members of the public each month with a standard letter referring the persons concerned to the option of civil proceedings. With the introduction of the new FADP, some of these enquiries will need to be handled directly.

Big data and artificial intelligence are increasingly establishing themselves as business models, and the FDPIC is required to provide supervision in an increasingly large number of domains due to growing technical risks to privacy. This means that the number of large data-processing projects run by businesses and state authorities is set to continue to grow.

Table 8: Consultancy for large-scale projects in 2022

Fundamental rights	1
Legislation - new FADP	2
Commerce and economy	1
Digital transformation	4
Total	8

Supervision

The dynamics of cloud-based applications mean that inspections now have to be carried out quickly. The increasingly fast pace of work and the growing importance of combining technical and legal expertise mean that long interruptions to investigations are no longer feasible, and several employees are required to manage more thorough inspections. During the year under review, 15.1% of resources were allocated

to inspections and supervisory duties, in line with the low average for the reporting years from 2015 onwards. Our 2023 inspection plan shows that twelve comprehensive inspections can be carried out with these resources. Now that more staff has been provided over the past two reporting periods to deal with data protection issues in preparation for the entry into force of the new FADP, the FDPIC plans to gradually increase the frequency of inspections of the federal bodies, the approximately 12 000 large and medium-sized companies and the approximately 10 000 foundations and associations 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. In the year under review, we were called on to participate in 383 office consultations.

Complete revision of the Federal Act on Data Protection

In the run-up to the entry into force of the new FADP and the corresponding implementing ordinance, the FDPIC has extensive preparatory work in view of his new duties and powers and in order to inform people and companies in good time. With the additional staff recruited, this work will be gradually completed as planned from early summer 2023 onwards.

Services and resources in the field of freedom of information

During the year under review, as we neared the tail end of the pandemic, the number of mediation requests remained consistently high (see Section 2.3). Parliament's approval on 8 December 2022 of the three posts for the FDPIC that had been envisaged in the dispatch on the Freedom of Information Act but had never been granted by the Federal Council has allowed the headcount in the Freedom of Information unit to be increased from 4.4 to 6 FTEs. The FDPIC will ensure that the processing backlogs caused by the pandemic and understaffing are gradually reduced over the coming reporting periods. Whether and how quickly this can be achieved will also depend on the number of mediation requests received in the future.

Participation in committee consultations and parliamentary committee hearings

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

- February 2022: SSHC-S on the Swisstransplant issue;
- February 2022: PIC-N on digital platforms;
- April 2022: PIC-N on the revision of the ordinance to the new FADP;

- June 2022: FDJP/FCh subcommittee of the CC-N on the Annual Report;
- October 2022: SSHC-N and PIC-N on the revision of the HIA and cost-containing measures;
- October 2022: EATC-N on the complete revision of the Customs Act;
- October 2022: FC-S and FC-N subcommittees on the 2023 budget;
- November 2022: SPC-N on the complete revision of the Customs Act;
- January 2023: LAC-N on the complete revision of the Customs Act;
- February 2023: FDJP/FCh subcommittee of the CC-S on implementation of the FoIA;
- March 2023: LAC-N on the federal act on the platforms for electronic communication in the judiciary;

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 that the FDPIC provides for individuals and for businesses and federal authorities running projects involving sensitive data meets general expectations. The FDPIC uses tools appropriate to the digital world.
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 and has a modern, user-friendly website. The new Federal Act on Data Protection introduces new reporting obligations and changes to existing ones. Reports can be sent to the FDPIC at any time via a secure, user-friendly reporting portal. This also helps reduce media discontinuity, making for more efficient processing.
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.

3.2 Communication

Figures

During the year under review, the FDPIC published six media releases, which can be found on the federal government's media portal, and twelve short statements. Media monitoring (covering a selection of key Swiss press and online media and key international printed publications) recorded just under 6000 posts last year, confirming the trend of the previous year, when we saw a sharp rise compared with the year before that (see 29th Annual Report, Section 3.2). The FDPIC's communications team answered around 300 media enquiries. These focused mainly on data transfer (approx. 100 enquiries), cyber security (45), surveillance (30) and regulation projects (15) such as chat control and the new federal act on customs and border security. In addition, we answered 12 media enquiries concerning the Freedom of Information Act.

The number of enquiries and tips from citizens in this reporting year is 6200, which is almost the same as last year (6600), when we saw a sharp increase of over 50 percent.

Main focus areas

Based on the media enquiries we received during the reporting period and the communication activities we carried out, we can conclude the following: The health sector remains at the centre of public interest in the wake of the coronavirus pandemic, which raised many questions about data protection, particularly with regard to contact tracing and the issue of Covid certificates. Investigative journalists identified data security vulnerabilities in medical registers, and cybercriminals gained unauthorised access to patient data that was stored on the servers of hospitals and doctors' surgeries without adequate security measures in place.

The sensitive health data of individuals was compromised in the national organ donor and breast implant registers, as occurred the previous year with the electronic vaccination register of the meineimpfungen.ch foundation (see 29th Annual Report, Section 1.4). The FDPIC launched a formal investigation in both cases (see Section 1.4). The Swisstransplant Foundation took on board most of the recommendations made in the FDPIC's investigation report and took the national organ donor register offline. The report on the breast implant register

is still pending. Meanwhile, the register has been taken offline for the time being.

We issued media releases on the Swisstransplant case both when the investigation was launched in January and when the final report was published in October. Straight after the hacker attacks on doctors' surgeries in the French-speaking part of Switzerland were discovered, the FDPIC contacted the surgeries in question in order to ensure that the patients concerned were promptly and fully informed. We published a short statement on this on our website on 31 March 2022. The FDPIC has expressed his views in the media on several occasions on the problem of inadequate security in the storage of health data.

After bankruptcy proceedings were started against the meineimpfungen. ch foundation at the end of 2021 and it

was announced in May 2022 that the bankruptcy office in charge intended to sell the vaccination data, the FDPIC initially demanded that the data be deleted but then later facilitated an attempt by the Department of Health of the Canton of Aargau to recover the data. We commented on this matter in a media release (see Section 1.4).

In the year under review, the intense public interest in medical data also in relation to the principle of freedom of information was particularly evident in connection with vaccine contracts. In his recommendation of 29 July 2022, the FDPIC urged the FOPH to disclose its vaccine contracts, which it did but with large sections blacked out, prompting public criticism.

Data sharing and trading

In addition to the medical registers, this year we focused on the cloud issue and the transfer of personal data to third parties in the commercial sector. We issued a detailed statement on the outsourcing of personal data by Suva to a Microsoft cloud and published

a short statement on this on 13 June 2022. We also commented in the media on the Federal Administration's cloud strategy (see 29th Annual Report, Focus II).

The FDPIC is currently reviewing a US lawsuit against Oracle America Inc. for unlawful tracking of internet users and issued a short statement on 27 September (see Section 1.3). The fact that data sharing and personal tracking are used not only for commercial purposes but also for state surveillance was demonstrated by the Qatari app required by the state during the 2022 World Cup. This prompted the FDPIC to issue a short statement advising travellers to Qatar for the World Cup to carry a second smartphone with them. The FDPIC takes a critical view of the EU chat-control project, another topic covered by the media during the year under review.

On Data Protection Day 2023, we drew attention to the recently revised guidelines on the processing of personal data in connection with elections and votes. These guidelines are relevant for federal and cantonal projects alike.

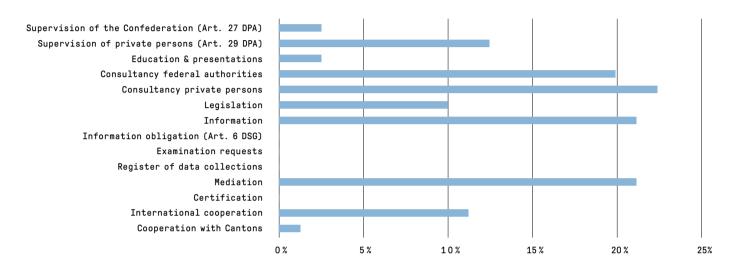
New website

Our media team was faced with the dual challenge of redesigning our website and preparing this annual report at the same time. The new website not only contains updated information on the new data protection act due to come into force on 1 September 2023 but has also been streamlined and reorganised to enable users to quickly find the information they are looking for. The new website also provides quick access to the three new reporting portals, namely DataReg for federal bodies to register their data processing records, the portal for reporting data security breaches, and the portal for registering data protection officers.

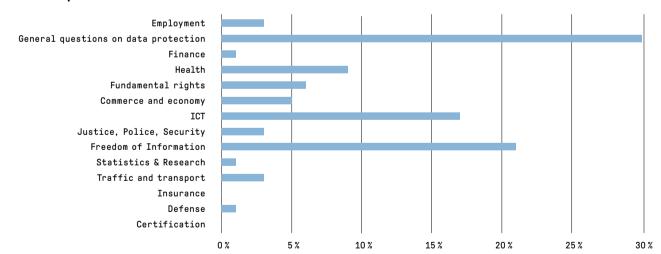
3.3 Statistics

Statistics on FDPIC's activities from $\mathbf{1}^{\text{st}}$ April 2022 to 31 March 2023 (Data protection)

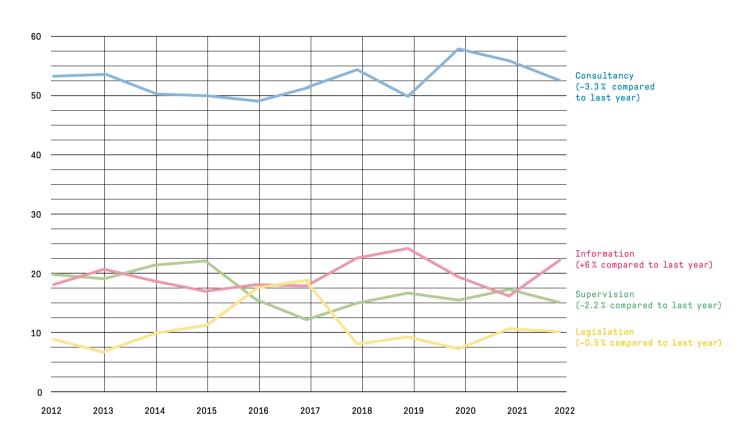
Workload per tasks



Workload per material



Multi-year comparison (as a percentage)



Overview of applications from $\mathbf{1}^{\text{st}}$ January to 31 December 2022

<i>*</i>	ķ			indieze i v		ompletely	·	rtially not	8	^		cedue st.	,	cument avai
Department	winder of	x ⁵	rccollag	xed xed	rccess ;	,eg	rce day	redis	Redusity	dram.	Pendi	ing ledinger.	40 80	cume
FCh	37		23		5		3		1		5		0	
FDFA	164		83		18		29		8		10		16	
FDHA	207		73		15		73		14		14		18	
FDJP	80		42		9		9		4		1		15	
DDPS	295		237		17		18		3		5		15	
FDF	110		37		15		23		10		15		10	
EAER	119		56		11		26		7		8		11	
DETEC	162		68		8		55		6		11		14	
OAG	6		5		1		0		0		0		0	
PS	0		0		0		0		0		0		0	
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	(24)	48	(3)	78	(7)	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)		-
Total 2012 (%)	518	(100)	230	(44)	140	(27)	123	(24)	19	(4)	6	(1)	-	-

Statistics on applications for access under the Freedom of Information Act from $\mathbf{1}^{\text{st}}$ January to 31 December 2022

			Ġ	Junit ted rears	letely .c	lerejy x	lally pended		
		Williag of Santages	is they it be	Shritted sees on the strong of	betally kccess come	rce diarre	Lail'y Reduest hor	Perdired les	uo availe
Federal Chancellery	FCh	22	0	14	3	3	0	2	0
FCh	FDPIC	15	0	9	2	0	1	3	0
	Total	37	0	23	5	3	1	5	0
Federal Departement	FDFA	164	0	83	18	29	8	10	16
of Foreign Affairs FDFA	Total	164	0	83	18	29	8	10	16
Federal Departement of Home Affairs									
FDHA	GS FDHA	10	0	2	2	1	0	2	3
	FOGE	4	0	3	0	0	0	1	0
	FOC	8	0	5	1	1	1	0	0
	SFA	2	0	1	0	0	1	0	0
	METEO CH	1	0	1	0	0	0	0	0
	NL	0	0	0	0	0	0	0	0
	FOPH	91	0	22	3	44	8	8	6
	FOS	4	0	1	2	1	0	0	0
	FSI0	11	0	11	0	0	0	0	0
	FSV0	27	0	14	3	8	0	0	2
	SNM	0	0	0	0	0	0	0	0
	SWISS MEDIC	45	8	10	3	18	4	3	7
	SUVA	4	1	3	1	0	0	0	0
	compenswiss	0	0	0	0	0	0	0	0
	Total	207	9	73	15	73	14	14	18
Federal Department	GS FDJP	6	0	4	0	0	0	0	2
of Justice and Police	F0J	22	0	9	2	1	0	0	10
FDJP	FEDPOL	12	0	5	4	3	0	0	0
	METAS	3	0	3	0	0	0	0	0
	SEM	24	0	13	2	3	2	1	3
	PTSS	0	0	0	0	0	0	0	0
	SIR	3	0	3	0	0	0	0	0
	IPI	4	0	2	0	2	0	0	0
	FGB	3	0	1	0	0	2	0	0
	ESchK	0	0	0	0	0	0	0	0
	FAOA	1	0	1	0	0	0	0	0
	ISC	1	0	1	0	0	0	0	0
	NKVF	1	1	0	1	0	0	0	0
	Total	80	1	42	9	9	4	1	15

			ē	outhit years	Jekejy	Jekejy	ially nded		
		Wille of	xhar in he	Antitude confinite	petalit d kcceleried	Lore of anti-	jaliseenu disuseenu Redusiitidi	Pending Pending	wo downers ho
Federal Department of Defence,	GS DDPS	33	1	6	7	11	1	1	7
Civil Protection and Sport	Defence	3	0	2	0	0	0	0	1
DDPS	FIS	21	0	5	7	5	0	0	4
	OA-IA	0	0	0	0	0	0	0	0
	armasuisse	10	0	3	1	0	0	4	2
	FOSPO	220	0	218	2	0	0	0	0
	FOCP	4	0	1	0	2	0	0	1
	swisstopo	4	0	2	0	0	2	0	0
	OA	0	0	0	0	0	0	0	0
	Total	295	1	237	17	18	3	5	15
Federal Departmemt of Finance	GS FDF	36	2	8	3	17	2	0	6
FDF	FFA	1	0	0	0	0	0	0	1
	FOPER	4	0	4	0	0	0	0	0
	FTA	11	0	5	3	2	0	0	1
	FCA	30	6	8	6	2	3	11	0
	FOBL	7	0	4	0	0	0	3	0
	FOITT	4	0	2	1	1	0	0	0
	SFA0	11	1	2	2	0	5	0	2
	SIF	3	0	1	0	1	0	1	0
	PUBLICA	1	0	1	0	0	0	0	0
	CCO	2	0	2	0	0	0	0	0
	Total	110	9	37	15	23	10	15	10

			,	buixxed rears	exejy	exelt .	all ended		
		with reduest	s weed in	Dhit ted as como	Access comp	kcce diang	al general Request hat?	Pending est	s No dounari
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	10	0	3	4	1	0	0	2
	SECO	37	0	11	4	9	3	4	6
	SERI	4	0	2	0	0	0	0	2
	FOAG	15	1	9	0	5	1	0	0
	Agroscope	0	0	0	0	0	0	0	0
	FONES	9	0	3	0	4	0	2	0
	FH0	1	0	0	0	1	0	0	0
	PUE	1	0	1	0	0	0	0	0
	COMCO	22	0	15	1	4	1	1	0
	ZIVI	2	0	2	0	0	0	0	0
	FCAB	7	0	7	0	0	0	0	0
	SNSF	0	0	0	0	0	0	0	0
	SFIVET	0	0	0	0	0	0	0	0
	ETH Board	9	0	3	1	2	2	1	0
	Innosuisse	2	0	0	1	0	0	0	1
	Total	119	1	56	11	26	7	8	11
Federal Department of the Environ- ment, Transport, Energy and Communications DETEC	GS DETEC	9	1	3	1	2	0	0	3
	FOT	6	0	1	2	2	0	_	
	FOCA					-	U	0	1
52.20	POCA	19	0	11	2	3	0	3	0
22.20	SF0E	19 25	0	11 5					
22.20	SFOE FEDRO	25 11			2	3	0	3	0
22.20	SFOE FEDRO OFCOM	25 11 19	0 0 1	5 4 8	2 1 0	3 18 1 6	0 0 1 0	3 0 2 1	0 1 3 4
	SFOE FEDRO OFCOM FOEN	25 11 19 62	0 0 1 1	5 4 8 34	2 1 0 0	3 18 1 6 18	0 0 1 0 5	3 0 2 1	0 1 3 4 2
	SFOE FEDRO OFCOM FOEN ARE	25 11 19 62 0	0 0 1 1	5 4 8 34 0	2 1 0 0 2	3 18 1 6 18	0 0 1 0 5	3 0 2 1 1	0 1 3 4 2
	SFOE FEDRO OFCOM FOEN ARE ComCom	25 11 19 62 0	0 0 1 1 0	5 4 8 34 0	2 1 0 0 2 0	3 18 1 6 18 0	0 0 1 0 5 0	3 0 2 1 1 0	0 1 3 4 2 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI	25 11 19 62 0 0	0 0 1 1 0 0	5 4 8 34 0 0	2 1 0 0 2 0 0	3 18 1 6 18 0 0	0 0 1 0 5 0	3 0 2 1 1 0 0	0 1 3 4 2 0 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI PostCom	25 11 19 62 0 0 8	0 0 1 1 0 0 3	5 4 8 34 0 0 2	2 1 0 0 2 0 0 0	3 18 1 6 18 0 0 4	0 0 1 0 5 0 0	3 0 2 1 1 0 0 2	0 1 3 4 2 0 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI PostCom ICA	25 11 19 62 0 0 8 0	0 0 1 1 0 0 3 0	5 4 8 34 0 0 2 0	2 1 0 0 2 0 0 0 0	3 18 1 6 18 0 0 4 0	0 0 1 0 5 0 0 0	3 0 2 1 1 0 0 2	0 1 3 4 2 0 0 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI PostCom ICA FPI	25 11 19 62 0 0 8 0 2	0 0 1 1 0 0 3 0 0	5 4 8 34 0 0 2 0 0	2 1 0 0 2 0 0 0 0 0	3 18 1 6 18 0 0 4 0 0	0 0 1 0 5 0 0 0	3 0 2 1 1 0 0 2 0 2	0 1 3 4 2 0 0 0 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI PostCom ICA FPI SUST	25 11 19 62 0 0 8 0 2 0	0 0 1 1 0 0 3 0 0 0	5 4 8 34 0 0 2 0 0 0	2 1 0 0 2 0 0 0 0 0	3 18 1 6 18 0 0 4 0 0	0 0 1 0 5 0 0 0 0	3 0 2 1 1 0 0 2 0 2 0	0 1 3 4 2 0 0 0 0 0
	SFOE FEDRO OFCOM FOEN ARE ComCom ENSI PostCom ICA FPI	25 11 19 62 0 0 8 0 2	0 0 1 1 0 0 3 0 0	5 4 8 34 0 0 2 0 0	2 1 0 0 2 0 0 0 0 0	3 18 1 6 18 0 0 4 0 0	0 0 1 0 5 0 0 0	3 0 2 1 1 0 0 2 0 2	0 1 3 4 2 0 0 0 0

			Winder of earlest	that it beg	phitted for company of the company of the control o	etely hccess comp	etely peres partie	allynded Leurended Redustration	Politica log	s dementable
Office of the Attorney General	OAG		6	0	5	1	0	0	0	0
OAG		Total	6	0	5	1	0	0	0	0
Parliamentary Services	PS		0	0	0	0	0	0	0	0
PS		Total	0	0	0	0	0	0	0	0
	T	otal sum	1180	27	624	99	236	53	69	99

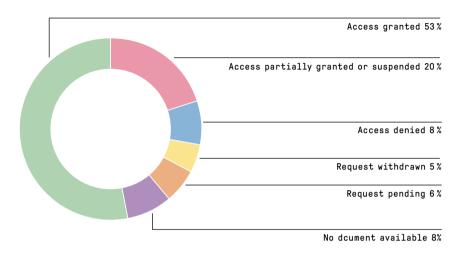
Requests for access 2022 with Corona reference

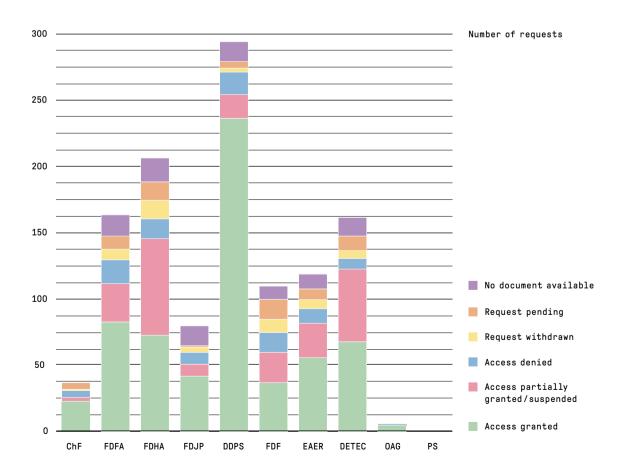
		.×.	r co _{uce}	exely	lekeji ^y	allyended		
		Reducate a second	kerence Serences comp	kccess conf	kcce of partiel	a La La Reduest Hutan	h beuging est	No doubert alle
Federal Chancellery	Total	0	0	0	0	0	0	0
FCh								
Federal Departement	Total	0	0	0	0	0	0	0
of Foreign Affairs FDFA								
Federal Departement	FOC	1	1	0	0	0	0	0
of Home Affairs FDHA	FOPH	57	18	2	22	3	6	6
	swissmedic	18	4	0	6	4	2	2
	Total	76	23	2	28	7	8	8
Federal Departmemt of Finance	GS FDF	6	0	0	5	0	0	1
FDF	FTA	1	0	0	1	0	0	0
	FOITT	2	1	0	1	0	0	0
	SFA0	1	0	1	0	0	0	0
	Total	10	1	1	7	0	0	1
Federal Department	Total	0	0	0	0	0	0	0
of Justice and Police FDJP								
Federal Department	OFCOM	1	1	0	0	0	0	0
of the Environment, Transport, Energy	Total	1	1	0	0	0	0	0
and Communications DETEC								
Federal Department	FOCP	1	0	0	0	0	0	1
of Defence, Civil Protection and	Total	1	0	0	0	0	0	1
Sport DDPS								
Federal Department	SECO	5	4	1	0	0	0	0
of Economic Affairs, Education and	Total	5	4	1	0	0	0	0
Research EAER								
Office of the Attorney General OAG	Total	0	0	0	0	0	0	0
Parliamentary	Total	0	0	0	0	0	0	0
Services PS								
	Total	93	29	4	35	7	8	10

Number of requests for mediation by applicant category

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

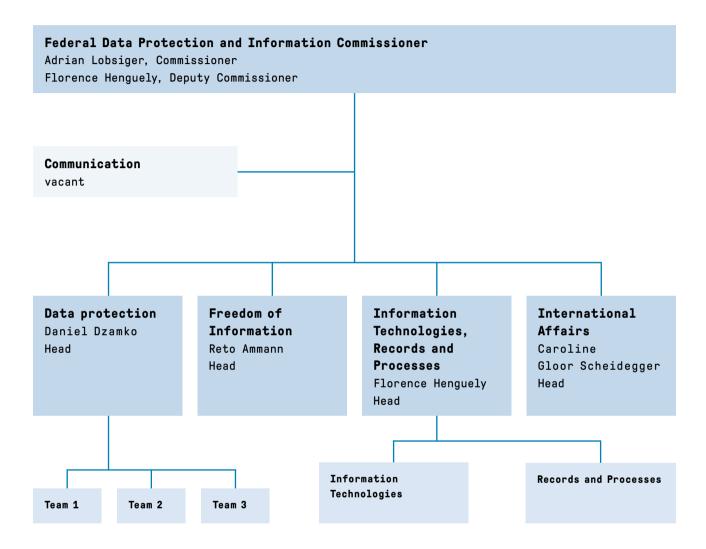
Applications for access in the federal administration from $\mathbf{1}^{\text{st}}$ January to 31 December 2022





3.4 Organisation FDPIC (Status 31 March 2023)

Organisation chart



Employees of the FDPIC

Number of employees	41		
FTE	34.1		
per gender	Women	20	49 %
	Men	21	51 %
by employment level	1-89 %	31	76%
	90-100%	10	24%
by language	German	32	78%
	French	8	20 %
	Italian	1	2 %
by age	20-49 years	24	59%
	50-65 years	17	41 %
Management	Women	4	40 %
	Men	6	60 %

Abbreviations

Al Artificial Intelligence	EDPS European Data Protection Supervisor	NaDB National data management programme
APA Federal Act on Administrative Procedure	E-ID Electronic Identity	NCSC National Cyber Security Centre
ArchA Federal Act on Archiving	EPR Electronic Patient Record	nFDPA new Federal Act on Data Protection
FOCBS Federal Office for Customs and Border Security	EPRA Federal Act on the Electronic Patient Record	NODR National Organ Donation Register
DataReg Register of data collections	FADP Federal Act on Data Protection	PNR Passenger Name Records
DPCO Ordinance on Data Protection Certification	Fedpol Federal Office of Police	Privatim Association of Data Protection Commissioners of the Swiss cantons
	FIS Federal Intelligence Service	
DPIA Data Protection Impact Assessment	FolA Freedom of Information Act	SAS Swiss Accreditation Service
DPO Ordinance to the Federal Act on Data Protection	GDPR General Data Protection Regulation	SDPA Application of the Schengen Acquis in Criminal Matters (SR 235.3)
DTI Digital Transformation and ICT Steering Sector of the Federal Chancel-	GPA Global Privacy Assembly	SIS II Schengen Information System of the 2 nd generation

ICT Information and Communication

Technology

lery

EDPB European Data Protection Board

VIS Visa Information System

Figures and tables

Figures	Tables
Figure 1: Evaluation of requests for access – trend since 2009	Table 1: Amicable outcomesp. 69
	Table 2: Processing time of mediation
Figure 2: Fees charged since the FoIA entered into forcep. 67	proceduresp. 70
	Table 3: Pending mediation
Figure 3: Mediation requests since the FoIA entered into force	proceduresp.71
	Table 4: Special provisions under
	Art. 4 Foldp. 80
	Table 5: No special provisions under
	Art. 4 FoIAp. 81
	Table 6: Staff positions available for
	FADP issuesp. 85
	Table 7: Services in data protection p. 86
	Table 8: Consultancy for large-scale
	projects in 2022p. 86
	Table 9: Outcome objectives
	for EDDIC p. 97

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. 410.030.ENG

Layout: Ast & Fischer AG, Wabern

Photography: Joël Stäheli

Characters: Pressura, Documenta Print: Ast & Fischer AG, Wabern

Paper: PlanoArt®, woodfree bright white



Key figures

Workload data protection

53%

15%

22%

10%

Consultancy

Supervision

Information

Legislation

Applications for access Freedom of Information (FoIA)

53%

5%

granted

partially granted or suspended

pending

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

applicable data.

The processing takes place with





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.





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.

Data security

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

 $\label{lem:commissioner} Federal \, Data \, Protection \, and \, Information \, Commissioner \, \\ Feldeggweg \, 1 \, \\ CH-3003 \, Bern \, \\$

E-Mail: info@edoeb.admin.ch Website: www.thecommissioner.ch

y @derBeauftragte

Phone: +41 (0)58 462 43 95 (Mo-Fr, 10 am - 12 pm)

Fax: +41 (0)58 465 99 96