28th Annual Report 2020/21

Federal Data Protection and Information Commissioner

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Annual Report 2020/2021

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 2020 and 31 March 2021.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Foreword

This reporting period was characterised by the ongoing COVID-19 pandemic and measures taken by the Federal Council and its administrative bodies to protect the population and support the economy.

Therefore, it will come as no surprise that our data protection authority's supervisory activities focused on the digital tools employed in the fight against the pandemic such as the SwissCovid App and the vaccination, test and recovery certificates. The pandemic was also the focus of our daily work of implementing the Freedom of Information Act as a large portion of the mediation requests we received concerned access to official documents such as those relating to the procurement of masks or vaccines.

While the State interfered in the privacy and informational self-determination of the population with the introduction of measure after measure in the fight against the persistent pandemic, our authority constantly insisted on the transparency of the State's actions. The Administration has to set priorities when dealing with crises, and so we adopted a pragmatic approach. For example, we encouraged members of the media to be patient regarding additional documentation of the activities of the Federal Office of Public Health.

It is too early to quantify the damage caused by this freedom-robbing pandemic, but one thing is certain: our authority has also learnt its lessons from the digital glitches during the crisis that caused astonishment and indignation. However, the criticism of the authorities and leaders should not obscure the shortcomings regarding the asynchronous digitalisation of our country, in particular the lack of an officially recognised electronic identity – a basic service – which has proven to be indispensable for up-to-date, privacy-compliant health data management.

Adrian Lobsiger
Federal Data Protection and Information Commissioner

Bern, 31 March 2021

Current Challenges 6

Data protection

1.1 **Digitalisation and fundamental rights** ... 14
- Data protection impact assessment of SwissID
- Swiss media publishers' single sign-on project for online portals
- Cloud initiatives for implementation of the federal ICT strategy
- Privacy compliance paramount in the Federal Administration's migration to the cloud
- The FOPH's access to Swisscom mobility data
- National data management programme
- Data processing by dating apps
- FDPIC to launch new reporting platforms

Focus I 22

The new Swiss Federal Act on Data Protection from the FDPIC's perspective

1.2 **Justice, Police, Security** 28
- Information requests received by the Federal Intelligence Service (FIS)
- Federal Council adopts dispatch on revision of the DNA Profiling Act
- Bill on checking of mobile phones in the asylum procedure
- FDPIC intervenes in the Federal Customs Administration: data processing inadequately regulated in the new customs police act

1.3 **Taxation and Finance** 31
- The FDPIC advocates the right to information in international tax-related administrative assistance before the Federal Supreme Court

1.4 **Commerce and economy** 33
- Investigations into the implementation of 5G by Sunrise and Swisscom
- Incorrect database entries at debt collection firm
- Car leasing credit checks
- Case investigation into Migros' video surveillance system
- Processing of customer data by online stores
- Use of Ricardo data within the TX Group
- Revision of the energy ordinance

1.5 **Health** 39
- Requirements for cloud services used to process patient data
- Data protection challenges of introducing facilitations for people who have been vaccinated
- Implementation of a data protection-compliant COVID-19 certificate
- Electronic patient records: First reference communities certified
- Swiss proximity tracing app (SwissCovid app)
- The legal framework for collecting contact details

1.6 **Employment** 47
- Permissibility of background checks in the application process
- Data protection aspects of working from home
- Data protection requirements for early detection of coronavirus in the workplace

1.7 **Insurance** 50
- Introduction of the HIS reporting and information system in the Swiss insurance business
- Transfer of membership data to sponsors
- Systematic use of the OASI number by the authorities: amendment of the law approved by Parliament

1.8 **Traffic and transport** 54
- Surge in enquiries from the public regarding drones
- Revision of the Passenger Transport Act: Avoiding discriminatory barriers for people travelling anonymously on public transport
- Use of airline passenger data to combat terrorism

Focus II 56

The Privacy Shield does not guarantee data subjects in Switzerland an adequate level of protection for data transfer to the US

1.9 **International** 58
- Introduction
- Council of Europe
- Global Privacy Assembly
- Adequate data protection post-Brexit
- Working group on the role of personal data protection in international development aid, international humanitarian aid and crisis management
- General Data Protection Regulation
- Supervision Coordination Groups on the SIS II, VIS and Eurodac information systems

Freedom of Information

2.1 **General** 66

2.2 **Requests for access – further increase in 2020** 68

2.3 **Mediation procedure – fewer mediation requests** 72
- Proportion of amicable outcomes
- Duration of mediation procedures
- Number of pending cases

2.4 **Legislative process** 76
- Legislative process for the transposition of the COVID-19 Loan Guarantees Ordinance into the COVID-19 Loan Guarantees Act
- Office consultation on the Federal Council's draft opinion on the National Council Political Institutions Committee report of 15 October 2020 on the Graf-Litscher parliamentary initiative 16.432. Charging system. Principle of freedom of information in the Federal Administration
- Revision of the Federal Act on the Promotion of Research and Innovation (RIPA). Office consultations in preparation for the Federal Council dispatch
- Partial revision of the HIA regarding cost-containment measures (Package 2)
- New Federal Act on General Aspects of the Collection of Charges and on Checks on the Cross-Border Movement of Persons and Goods by the Federal Office for Customs and Border Security (FOCBS Enforcement Task Act)

The FDPIC

3.1 **Duties and resources** 82
- The pandemic
- Services and resources in the field of data protection
- Participation in committee consultations and parliamentary committee hearings
- Services and resources in the field of freedom of information

3.2 **Communication** 87
- Communications dominated by the pandemic
- Communication challenges and conditions
- Media interest remains high
- Opinions, recommendations and publications

3.3 **Statistics** 90
- Statistics on FDPIC's activities from 1th April 2020 to 31 March 2021 (Data protection)
- Overview of applications from 1st January to 31 December 2020
- Statistics on applications for access under the Freedom FoIA from 1th January to 31 December 2020
- Requests for access 2020 with Corona reference
- Number of requests for mediation by categories of applicants
- Number of requests of the whole Federal Administration

3.4 **Organisation** 100
- Organisation chart
- Staff

Abbreviations 102

Figures and tables 103

Impressum 104

In the cover
- Key figures
- Data protection concerns

Texts and pictures with Corona reference

Current Challenges

I Digitalisation

The coronavirus pandemic – still ongoing despite the availability of vaccines – and the resulting accelerated digitalisation of work and consumption continued to characterise the use of information and communication technologies (ICT) in Switzerland during the year under review.

Technology and economy

The technical and economic potential for interference in individuals' privacy and right to self-determination remains great.

Today's digital world offers ultrafast transmission of signals via the internet which are then converted by billions of portable devices ("smart devices") into text, images, sound or vibrations, namely information perceptible to the senses. Information is constantly at our fingertips almost everywhere we go, satisfying our curiosity, gaming lust and thirst for knowledge.

However, people are quickly annoyed when their personal data is used for specific purposes or their privacy is invaded. Private individuals and companies typically protect and encrypt part of their data – a thorn in the side of police and executive administration. Furthermore, owners of smart devices are also increasingly being asked by private individuals and the authorities to present their devices for automated data comparisons ("scanning"). Some people are uneasy at the thought of providing access to their devices, which contain a vast amount of personal data providing an insight into their digital lifestyle. Therefore, not everybody is willing to produce a smart device equipped with a specific program installed on it. Others are unable to do so because of their age, health condition or disability.

At this stage of the fight against the pandemic, these people are likely to come under further pressure. With businesses reopening and bans on events being lifted, people may well be required to provide proof of vaccination against COVID-19 or a negative Covid test result to access certain goods and services. In order to prevent people from being obliged to carry a smartphone, the FDPIC demands that alternative methods be offered for collecting health data, in addition to digital methods, subject to reasonable terms. This is important as the systematic processing of personal data during the pandemic is likely to affect people's right to informational self-determination beyond the pandemic. Given the near-universal use of smart devices, the pandemic could well become a launch pad for government and commercial interests requiring these devices to be accessible at all times as a mobile means of identification and documentation. In order to prevent smart devices from degenerating into electronic tags, the Commissioner has publicly demanded that traditional information carriers such as paper also be permitted for both collecting contact data for contact tracing and providing proof of vaccination or a negative Covid test result.These considerations may well have played a crucial role in the federal legislator's decision to enshrine in the Epidemics Act in early summer 2020 the principle that access to services must not be made conditional on the use of the Swiss Covid app.

The far-reaching impact of increasing automation in the processing of large amounts of data were clearly demonstrated again this year in voting and elections. When machine and digital technology is used to process large numbers of votes, voters' main concerns are the transparency and reliability of the technology used and the issue of data protection. The widespread mistrust of automated processes also contributed to the turmoil following the recent US presidential elections. The White House lawyers at the time attacked the abstract, technical aspects of data transmission, counting and analysis, systemically discrediting them with general criti-

cism, thus fuelling public uncertainty. This was met with messages in online forums from people convinced that rigged algorithms and other schemes were at play. Consequently, as elections and voting become increasingly automated, we can expect instruments of modern data protection law that require a minimum of human intervention to become increasingly important in regulating automated decision-making processes in the future.

Society and data policy

On 7 March 2021, Swiss voters firmly rejected the Federal Act on Electronic Identification Services (E-ID). Despite a vain attempt by the Federal Council and Parliament to gain the people's trust in a private E-ID issuer, the committee responsible for the referendum prevailed with its key argument that issuing E-ID should be the exclusive responsibility of the authorities. The people's desire for more State leadership in a digital project of this scale is largely justified by their expectation that the State will act and process personal data in accordance with the provisions of the law and that the authorities will conscientiously abide by the principle of legality.

The people's expectations do not entirely tally with the FDPIC's experience: During our advisory and supervisory work, we noticed that, faced with the challenge of the digital transformation, the Federal Administration is increasingly struggling with the principle of legality and doubting the requirements of the Federal Supreme Court regarding the level of detail required for the legal basis governing the processing of personal data: For example, it is no longer acceptable for the content, categories, purposes, rate and duration of data processing by the authorities to be to enshrined in law as this is thought to promote the preservation of outdated "data silos" and "media discontinuity" that would prevent the Administration from networking flexibly and functioning efficiently.

It should be noted that the Commissioner does not question the digitalisation of the Federal Administration or the need for a modern legal basis that does not unnecessarily restrict the offices' freedom in organisational and technological matters. The FDPIC's solution-oriented approach to his advisory activities shows that general, abstract and technology-neutral legal provisions do not hamper digital transformation in any way. He also supports the Administration's efforts to streamline traditional system structures.

Despite this commitment to the digital transformation, the federal data protection supervisory authority cannot dispense the Administration from deriving the purpose, scope and rate of digital processing of personal data from a mandate of the political bodies enshrined in the law in a way that the general public can comprehend. It is

«The people shall not be obliged to carry a smartphone on them.»

also essential that the democratically legitimised legislator set political and constitutional jurisdictional boundaries when regulating the processing of personal data by the authorities by assigning responsibilities, restricting direct access to personal data and regulating the exchange of information for administrative assistance. The fact that the digital transformation of the Federal Administration is to be implemented without diluting the principle of legality is also clear in the new Federal Act on Data Protection, in which the 2020 legislator reiterated its promise that federal bodies would process sensitive personal data only if provided for by a law put to a referendum clearly setting out the purposes, extent, type and content of the data to be processed and the rate of data processing.

During the year under review, the FDPIC discussed the requirements of the principle of legality with the Federal Customs Administration among others. In particular, they discussed the scope for shaping the new Federal Office for Customs and Border Security, whose staff will process large amounts of sensitive personal data and, like the staff of the Federal Office of Police and the Federal Intelligence Service, is to be armed and have police powers.

The processing of personal data by these federal security authorities is associated with high risks for the privacy and informational self-determination of individuals as the authorities in question obtain some of their information covertly and impose severe coercive measures on data subjects depending on the outcome of their data analyses. Consequently, the federal data protection supervisory authority must not tolerate any compromises in the digital transformation of these offices with regard to compliance with the Federal Court requirements in terms of the level of detail required for the legislation governing the processing of personal data by the police authorities. Only laws that are sufficiently precise can prevent confusion over responsibilities during the digital transformation of the federal security authorities and the cantonal police force. Personal data is processed by the federal security authorities for a range of different purposes such as preventing danger, prosecuting criminals, protecting the state and enforcing numerous special laws. If the digital linking of such data were left to the discretion of the authorities, this would lead to a non-transparent concentration of police power that would be incompatible with the separation of powers enshrined in the Federal Constitution.

It is all the more important to restrict the processing of police data by the federal authorities by law to task-specific categories given that the federal security authorities, in their historically-rooted complexity, are organised very differently from their cantonal counterparts. While the covert and coercive collection of personal data at the cantonal level is carried out by a single police force whose duties and powers are set out in cantonal police law, the Confederation, as mentioned, divides its police power among a large number of armed agencies, which process personal data in accordance with a wide variety of federal laws. For many years now, the Commissioner has lamented in vain in his annual reports the fact that the lack of a piece of legislation comparable to the cantonal police laws and the overwhelmingly large number of special federal regulations effectively reduce the transparency of personal

«The federal security authorities are finding it increasingly difficult to deal with the principle of legality.»

data processing by the federal security authorities in a way that is difficult to justify with data protection legislation. Within the context of the digital transformation, this fragmentation of the law is making it increasingly challenging for the authorities to maintain an overview of their complex data processing activities. The Commissioner sees this as a further explanation as to why the federal security authorities in particular are finding it increasingly difficult to deal with the principle of legality.

Legislation

The Swiss Parliament has completed its extensive work of fully revising the Confederation's data protection legislation, which culminated in the fully revised Federal Data Protection Act of 25 September 2020 (see Focus 1).

II Consultancy, supervision and mediation

In his role as a supervisory authority, the FDPIC seeks to ensure that the extent of personal data processing is not solely driven by technical feasibility but is instead subject to legal restrictions. He therefore requires that providers of digital applications minimise privacy risks at the planning and project stage, document them and submit this documentation to the company and the federal data protection supervisory authority. With this approach, we continued to support many big data projects run by federal authorities and private companies and promoted the responsible use of modern working tools such as the data protection impact assessment as well as the employment of data protection officers within companies.

The FDPIC's main focus this year was on providing supervisory support and overseeing numerous digital projects relating to the fight against the coronavirus pandemic. These activities are marked in yellow in this annual report. The pandemic also challenged the FDPIC in his role as an information commissioner: this year he faced a large number of mediation requests relating to official documents regarding the procurement of masks and vaccines among others. After the Swiss government made working from home mandatory, the majority of these requests resulted in the time-consuming task of issuing written recommendations.

Six out of the 15 major projects that the FDPIC oversaw as part of his statutory advisory duties were related to the digital transformation of the Federal Administration ordered by the Federal Council. This involves reducing the digitalisation backlog pointed out by politicians and the media, caused mainly by the pandemic response. In addition to the above-mentioned projects of the Federal Office of Public Health, the FDPIC also oversaw the digitalisation projects of numerous other federal bodies, focussing, as mentioned, on the security authorities (see above and Sections 1.2 and 3.1).

After declining significantly in the 2015/16 period, expenditure on supervisory duties has increased again slightly in recent years, stabilising at a low level due to an ongoing lack of resources. This year, the FDPIC was again unable to meet justified public expectations sufficiently. Although the FDPIC is keen to work closely with the National Cyber Security Centre, he lacks the resources (see Section 3.1) to perform the systematic random technical security checks and inspections that would be especially useful for the storage of sensitive health data. In this context, it is worth mentioning the case of the Myvaccines foundation.

III National and international cooperation

National cooperation

The fight against the current coronavirus pandemic has raised questions about the extent of federal and cantonal jurisdiction in relation to contact tracing and the processing of personal data in connection with COVID-19 vaccination and testing. The long-standing relationship between the FDPIC and the cantonal data protection commissioners was instrumental in ensuring a coordinated and pragmatic approach.

International cooperation

The fight against the pandemic and the associated processing of health data raise similar issues for data protection authorities around the world. Therefore, the FDPIC has been closely monitoring international developments and has been in touch with his foreign data protection authority counterparts.

Council of Europe

The FDPIC is keen to actively participate in the Council of Europe. Accordingly, he participated again this year in the meetings of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). At the same time, a FDPIC representative was elected to the office of the Consultative Committee for Convention 108, which manages the Committee's work between plenary sessions.

Evaluation of the level of data protection

The EU Commission's report on the adequacy of the level of data protection in Switzerland was initially due to be published at the end of May 2020 but was delayed and is now expected before summer 2021.

During the year under review, Switzerland and the UK – which has now left the EU – achieved mutual recognition of an adequate level of data protection.

Swiss-US Privacy Shield no longer provides an adequate level of data protection

The Court of Justice of the European Union (CJEU) delivered its eagerly awaited judgment on the transfer of data from the EU to the US (Schrems II) on 16 July 2020, in which it declared invalid the EU Commission's adequacy decision 2016/1250 regarding US companies certified under the EU-US Privacy Shield regime.

CJEU judgments do not apply to Switzerland. However, based on his periodic evaluations of the CH-US Privacy Shield regime and the mutual recognition of adequacy between Switzerland and the EU, the FDPIC found that the regime no longer offers an adequate level of protection to data subjects in Switzerland. As a result, he advised Swiss companies to transfer data to the US on the basis of contractual guarantees and project-specific risk impact assessments.

Data protection

1.1 Digitalisation and fundamental rights

Data protection impact assessment of SwissID

During the year under review, SwissSign Group AG submitted its data protection impact assessment of SwissID to the FDPIC.

Given the systemic importance of SwissSign Group AG's "SwissID" product, the FDPIC had previously met regularly with the project managers, among other things to ensure that anonymous registration be allowed for pure single sign-on (SSO) services. SwissSign Group AG has incorporated this demand in its privacy policy. Its terms and conditions will be amended shortly.

After SwissSign Group AG appointed an external data protection officer to perform a data protection impact assessment, during the year under review the document was submitted to the FDPIC for evaluation. The document contained a detailed description of the firm's data processing activities, an evaluation of the risks associated with the measures relating to fundamental rights, and a list of privacy protection measures.

The FDPIC noted that, according to the data controller, the data protection impact assessment had been completed and that data processing carried out in connection with SwissID was considered legitimate based on the risks and measures described.

Swiss media publishers' single sign-on project for online portals

The Swiss Digital Alliance is pushing ahead with its work to create a single sign-on (SSO) solution for media publishers' online portals. The FDPIC has highlighted opportunities for improvement during an exchange.

The Swiss Digital Alliance has launched a single sign-on (SSO) project aimed at allowing users to log in with a single ID and password to access various web offerings of Swiss media companies. The Alliance – an association of Swiss media companies – further developed its project to create a centralised SSO system and launched a pilot test phase in spring 2021. During previous project presentations and an exchange on the subject, we expressed our view to the Digital Alliance on aspects of the project that were essential to ensure data protection and highlighted opportunities for improvement.

The project will continue beyond the end of the year under review, and we will continue to monitor the work carried out to ensure that the SSO system developed incorporates privacy protection into its design.

Cloud initiatives for implementation of the federal ICT strategy

The FDPIC oversaw the development of strategic goals and guidelines for the digital transformation of the Federal Administration. Development of the necessary IT infrastructure includes ensuring the safe use of public cloud services in addition to the existing option of running applications and processing data in the Federal Administration's own data centres (private clouds). We call for data protection requirements to be observed as early as the tendering stage.

Digitalisation requires the use of a large number of highly efficient, flexible and expandable applications and services. Both public and private cloud services are used in order to meet these requirements as they provide fast access to the necessary tools and services, acting as a self-service source (see separate box for definitions). The Federal Administration already uses a variety of easily expandable cloud services to a limited degree. According to a survey conducted in the federal departments and at the Federal Chancellery in the last quarter of 2019, the need for public cloud services in particular is set to increase in the future.

Public clouds allow the administrative units of the central Federal Administration to access innovative and relatively inexpensive solutions and the latest technologies quickly and efficiently. This opens up new opportunities for providing fast and efficient access to administrative digital services. At least in areas that are not subject to high security, costly ICT services can thus be optimised and outsourced. For that reason, the Federal Administration took the strategic decision of introducing public cloud services in addition to its existing private cloud services. Furthermore, a detailed study was needed to determine the needs, configuration, requirements and feasibility of a public, 100% Swiss-based cloud and data infrastructure ("Swiss Cloud").

However, the use of public cloud services creates a high level of dependence on providers, most of which operate internationally, in terms of both technological dependence and the availability of data and applications. This inevitably raises the question as to how to ensure sovereignty over one's own data and protection against data leaks.

The FDPIC addressed this issue by extending the criteria applied in the procurement of public cloud services in order to ensure that providers guarantee data protection and data security throughout the entire processing chain. He also played a leading role in drawing up guidelines for the admissibility of public cloud services from an information security and data protection standpoint. Given the scope of this project, the FDPIC also felt it crucial to demand specific data protection certifications from the providers as early as the tendering stage.

Data protection considerations clearly need to be taken into account at a very early stage in projects involving the processing of personal data. The FDPIC will continue to oversee cloud initiatives and will check to ensure that the specified criteria and requirements are observed.

Cloud services

Whereas in the past most companies used to have their own data centres, today they often rely on cloud services instead. Cloud computing (or "cloud" for short) refers to a service providing online access to data storage space, processing power and software. A cloud is therefore an online IT infrastructure to which data or entire IT environments are outsourced. Different cloud services are available depending on intended use and desired level of integration.

Clouds offer the following main advantages:

- High scalability, i.e. the ability to easily increase (or reduce) storage capacity and processing power as needed;
- High availability and security through the use of the latest technologies;
- Financial savings: the environment is maintained by the provider, eliminating the need for companies to invest heavily in their own server infrastructure.

Intended use of the cloud service

Cloud services offer various delivery models depending on the user's needs. The main models are the following:

- Private clouds: Private clouds are usually created within a company's own data centre and used by a single company. They are typically operated by the company itself or by an external provider and are accessible only to specific groups of people. Private clouds meet strict data security and data protection requirements and are therefore particularly suitable for sensitive data such as confidential personal information or confidential company data.
- Public clouds: These are services offered by freely accessible providers that offer their services to everyone via the internet. Here, users all share the same infrastructure. Well known online storage providers such as Dropbox or Google Drive and email providers such as Gmail or Hotmail typically rely on public clouds.
- Hybrid clouds: These are a combination of private and public clouds. Users have access to a public cloud which includes a private environment for sensitive data and applications. This mixed form is popular as it allows users to save highly sensitive data to a private cloud while less sensitive data can be outsourced more easily and cheaply.
- Multi-clouds: This is a concept that uses multiple cloud services from a variety of providers and offers a wider range of options compared with hybrid clouds.

Level of cloud integration

In cloud computing, a general distinction can be made between three cloud service levels, which build on each other. The three different layers – infrastructure, platform, and software – make up the cloud architecture.

- Infrastructure as a service: This model provides access to resources such as computing power, storage and network capacity via the cloud. While local servers were previously moved to the cloud, now cloud delivery replaces on-site hardware, leaving the company to provide support for operating systems and applications.
- Platform as a service: This model adds an operating system and system-level software such as backup, antivirus and maintenance software etc. via the cloud. Instead of developing software in their own environments, companies may use entire software development and delivery environments via the cloud.
- Software as a service: This model provides access to cloud-based software including all underlying IT infrastructure, platforms and components.

Privacy compliance paramount in the Federal Administration's migration to the cloud

The Federal Administration's cloud strategy aims to pave the way for cloud-based digitalisation of the Federal Administration. The FDPIC commented on the strategy paper and was able to voice some key data protection concerns.

The Federal IT Steering Unit (FITSU) was tasked by the Federal Council with drawing up a strategy document fleshing out the Confederation's cloud vision and setting out binding guidelines and principles governing the procurement of cloud applications by individual administrative units. The FDPIC received a preliminary version of the strategy document for pre-consultation and identified various points that could be improved. In particular, the FDPIC noted that the document focussed heavily on information security requirements while dealing only superficially with other legal aspects of data protection.

Therefore, we proposed amendments to the strategy document, setting out the data protection requirements for the outsourcing of data processing to a cloud. In particular, our proposed amendments sought to ensure that the additional risks of outsourcing data processing to foreign public cloud providers in countries that did not offer an adequate level of data protection were taken into account.

In this spirit, we suggested that the document specify the requirement for a data protection impact assessment to be carried out when personal data was processed in the cloud in order to assess whether or not data processing via cloud applications was permissi-

ble and, if so, with what measures in place. This mechanism is designed to help users verify the legal compliance of cloud applications based on server location, the law applicable in the country in question and the envisaged technical and organisational measures. Our comments and suggested changes have been incorporated into the final version of the document.

The Federal Administration and private users of public cloud services are increasingly grappling with this issue since the Privacy Shield Framework was re-evaluated (see Section Focus II of this report on the Privacy Shield) as standard contractual clauses cannot be assumed to guarantee an adequate level of data protection in the US – and most providers are US-based.

CORONA

The FOPH's access to Swisscom mobility data

After the Federal Council banned gatherings of more than five people in public places on 21.03.2020, the FOPH used information provided by Swisscom to verify compliance with this measure introduced to stop the spread of the coronavirus. The FDPIC concluded that Swisscom had only granted the FOPH access to anonymised data.

Swisscom uses the Mobility Insights Platform (MIP) to process anonymised group statistics based on aggregated mobility data in order to analyse mobility behaviour across Switzerland. After it became known that the Federal Office of Public Health (FOPH) was to be granted access to this data as part of the fight against the pandemic to determine whether or not people were still gathering in large numbers in Switzerland, the FDPIC launched a preliminary investigation into the matter, during which it also took a closer look at the FOPH.

The visualisations, made available with a delay of at least eight hours, show mobile phone owners' movements over time, identifying areas measuring 100 by 100 metres in which at least 20 mobile phones containing Swisscom SIM cards are present. Location data is anonymised and aggregated at the earliest possible stage, and the FOPH is never shown the plain data on which the visualisation is based. The visualisations accessible to the FOPH do not allow any conclusions to be drawn about specific individuals and are therefore anonymous. For that reason, in his brief evaluation of 03.04.2020, the FDPIC concluded that data processing by Swisscom and the subsequent transfer of anonymous data to the FOPH was permitted under data protection law (see our communication of 03.04.2020, not available in English).

Based on that information, the FDPIC did not need to open a formal fact-finding procedure. However, the FDPIC took the view that the information available to the public on the cooperation between Swisscom and the FOPH and on the associated data processing was insufficient and not readily accessible. He therefore called on Swisscom to provide the public with more detailed information on its data processing activities. Swisscom complied with his request and compiled a list of FAQs on the FOPH's use of Swisscom's Mobility Insights Platform.

National data management programme

Data management in the public sector needs to be simplified and streamlined by reusing data. To this end, the Federal Council has launched a number of pilot projects as part of the national data management programme. The FDPIC is working with the Federal Statistical Office, which is responsible for the programme, in order to ensure compliance with data protection regulations during implementation.

The national data management programme (NaDB) aims to implement a system whereby people and businesses are required to provide certain data to the authorities once only (referred to as the "once only" principle), thus reducing the burden on the data subjects. Likewise, data reuse is expected to reduce the administrative burden on the public administration. This can be achieved by facilitating data sharing between authorities.

As part of the office consultation procedure, the FDPIC first of all commented on the reports of four pilot projects on the quality assurance of business data, wage statistics and tax data and on the relevant processes, roles and responsibilities. He stressed the crucial importance of data protection in the reuse of data envisaged in the programme. In his view, data reuse poses serious risks to data protection. In particular, for example, it must be ensured that the "once only" principle does not lead to a widening of the circle of persons authorised to access the data. It is also crucial to regulate who is authorised to process what data and for what purpose. In addition, a clear distinction must be made between data processing for statistical purposes and data processing for other purposes. Furthermore, there must be transparency on how data is collected and processed and on how it may be accessed.

Following this office consultation, an exchange took place between the Federal Statistical Office – responsible for implementation – and the FDPIC during which these aspects were discussed again. The Commissioner will continue to oversee implementation of the NaDB programme in an advisory capacity and will remain available to the relevant bodies as a point of contact.

CORONA

Information sheet on the privacy-compliant use of audio and video conferencing systems

Audio and video conferencing applications experienced a surge in popularity during the coronavirus lockdown. The vast number of people using them has made the digital platforms on which they operate attractive to hackers. Therefore, when choosing software, information security and data protection should be top priorities. Sometimes personal data is improperly processed, data security is not always guaranteed, and the platforms themselves can have known vulnerabilities.

The FDPIC information sheet (see our communication "Measures for the safe use of audio and video conferencing systems") is aimed at all user groups, both in business and in private life, and provides tips on how to protect your personal data and avoid the undesirable consequences of data misuse. The FDPIC provides recommendations on how to protect your data when using such applications, for example when dealing with meeting IDs and passwords, using webcams or conducting screen presentations. The information sheet also provides guidance on how to evaluate and introduce an audio and video conferencing system. For example, it is advisable to verify the provider's handling of metadata, data encryption and data security. Furthermore, before introducing a system, companies should draw up rules for use. Finally, companies are obliged to clearly inform employees of any recording or monitoring.

Although it might be tempting to integrate the ad hoc solutions used during the pandemic in the existing ICT infrastructure, the Commissioner recommends following the standard procedures and relying on the expertise of IT managers for the procurement of such systems in order to ensure compliance. The audio and video-conferencing systems used should have security settings that ensure a high level of data protection, particularly with a view to protecting professional and commercial secrecy.

Data processing by dating apps

The FDPIC has initiated a procedure at a Swiss provider of dating apps to review its data processing methods and its handling of deletion requests.

According to the Federal Statistical Office, dating apps and websites are becoming increasingly popular ways to meet potential partners in Switzerland: almost twenty per cent of couples who started a relationship in the past five years met online via a dating site, dating app or social network[1]. Dating apps and websites identify suitable matches based on users' personal details, which are processed automatically or semi-automatically via an algorithm.

To increase the chances of finding a perfect match, users are encouraged to provide sometimes very sensitive information about themselves, for example relating to their ideology, religion and alcohol consumption, the processing of which involves high risks as it allows conclusions to be drawn about key aspects of the users' personality.

In spring 2021, the FDPIC opened a formal investigation at a dating app provider based in Switzerland after users alerted us to the fact that they had no way of deleting their accounts via the app and that requests for dele-

[1] Federal Statistical Office (issuer): Families and generations survey 2018. Initial results. Neuchâtel 2019, p. 9. https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/erhebungen/efg.assetdetail.10467788.html (accessed on 14.04.2020)

tion addressed to the operator of the app were not being processed. As well as clarifying this aspect, during our investigation we aim to verify the provider's compliance with other data protection requirements as well, particularly in terms of transparency and security of the data processed as well as any transfer of personal data to third parties.

FDPIC to launch new reporting platforms

The FDPIC is preparing to launch two online platforms for reporting data loss and publishing the contact details of data protection officers as required by the new Federal Act on Data Protection. The revised FADP introduces new obligations for data controllers to report to the FDPIC. These obligations include registration of data processing activities by federal bodies, publication of the contact details of data protection officers and notification of data security breaches. The platforms are designed to minimise user effort by providing safe, simple online reporting tools.

The FDPIC's register of data files is to be modified as only federal bodies will be required to register their lists of data processing activities with the Commissioner in the future. The search and reporting platform www.datareg.admin.ch will be updated accordingly to meet the new requirements.

In addition, two new reporting platforms are to be launched. One platform will provide an efficient, well-structured tool for data controllers to register appointed data protection officers. The platform will operate on a self-service basis, allowing data controllers to enter, modify and delete the contact details of data protection officers directly. The other platform will be for notification of data security breaches that pose a serious risk to the data subjects. The Commissioner expects a large number of notifications. This platform, too, will be well-structured and user friendly and offer efficient automated data analysis. It is designed to provide a real-time response to reported events.

The new Swiss Federal Act on Data Protection from the FDPIC's perspective

The private sector and federal authorities need to bring their processing of personal data into line with the new provisions of the revised Swiss Federal Act on Data Protection (FADP) before the latter comes into force (see box). In February 2021, the Commissioner noted and published the most significant changes in his view (see press release "The new FADP from the FDPIC's perspective"), highlighting several points that need to be considered.

Only data of natural persons

Similarly to the EU General Data Protection Regulation (GDPR), the revised FADP sets out to protect only the privacy of natural persons about whom personal data is processed, no longer including the data of legal entities.

Sensitive personal data

The current definition of sensitive personal data has been extended to include genetic data and biometric data provided the latter can uniquely identify a natural person.

Privacy by design and by default

The revised FADP enshrines the principles of privacy by design (data protection through technology) and privacy by default (data protection through privacy-friendly default settings). These principles require authorities and businesses to implement the processing principles set out in the FADP from the planning stage. Applications are to be designed in such a way that data is anonymised or deleted by default. Privacy by default protects users of private online offerings who have not looked into the terms of use or the associated right of objection as only the data that is absolutely necessary for the intended purpose is processed, as long as users do not take action and allow further processing.

Data protection impact assessment

Data protection impact assessments are nothing new in Swiss data protection law: federal bodies are already required to conduct them. If the planned processing may involve a high risk to the privacy or the fundamental rights of data subjects, under Art. 22 revFADP, data controllers from the private sector must now also carry out a prior data protection impact assessment. The high risk comes from the nature, scope, context and purposes of processing, particularly when using new technologies. In particular, processing is deemed high risk if profiling or extensive processing of sensitive data is planned. If a data protection impact assessment reveals that the planned processing still results in a high risk to the privacy or fundamental rights of data subjects, despite the measures envisaged by the data controller, under Art. 23 revFADP the data controller must seek a prior opinion from the FDPIC. If the FDPIC objects to the impact assessment itself, it will suggest relevant clarifications or additions to the data controller.

Codes of conduct

Art. 11 of the new FADP provides incentives for professional, trade and business associations to develop their own codes of conduct and to submit them to the FDPIC for an opinion. The FDPIC's opinions are then published. They may contain objections and recommend relevant modifications or clarifications. Positive opinions from the FDPIC justify the legal assumption that the conduct set out in the code complies with data protection laws. However, codes of a general nature cannot absolve organisations of responsibility for any risks that the text fails to describe in detail.

Certifications

Under Art. 13 revFADP, besides the operators of data processing systems or programs, manufacturers can now also have their systems, products and services certified. Certification enables businesses among other things to provide evidence that they comply with the principle of privacy by default and that they have an appropriate data protection management system in place.

List of data processing activities

Under Art. 12 revFADP, both data controllers and data processors are now required to keep a list of all data processing activities. The new FADP sets out the minimum details. The list must always be kept up to date. In the ordinance, the Federal Council will set out exemptions

for businesses with fewer than 250 employees and where data processing entails a low risk of privacy breaches for data subjects.

Cross-border disclosure of personal data

Under Art. 16, the revised FADP stipulates that data may be disclosed abroad if the Federal Council has ascertained that the legislation in the third country guarantees adequate protection. It will publish a list for this purpose which was compiled by the FDPIC under the previous law. If the relevant export country does not feature on the Federal Council's list, data may still be transmitted there (as under the previous law) if adequate data protection can be guaranteed by other means.


ABHOLEN / PICK UP

If data is to be disclosed abroad – including storage on foreign systems (cloud) – the countries in question are to be indicated regardless of whether or not these offer adequate data protection. Here the FADP goes further than the GDPR.

Extended duties to provide information

In line with the revision's objective of promoting transparency, Art. 19 revFADP extends the duty of businesses to provide information. Under the new legislation, a private data controller must appropriately inform data subjects in advance every time personal data is collected, even if the data is not collected by them directly. In the current FADP, this duty to provide information is only stipulated for sensitive personal data and personality profiles. Businesses will have to review and update their privacy policies accordingly. If the data processing results in automated individual decision-making, under Art. 21 revFADP, data controllers have new duties to provide information to complainants, and to grant them the consultation and inspection rights to which they are entitled.

Right of data subjects to information

The right of data subjects to request information about whether data about them is being processed has been extended in the new FADP. Art. 25 revFADP contains an extended list of minimum information that data controllers must disclose, such as how long processed personal data is stored.

Obligation to report data security breaches

Under Art. 24 revFADP, the controller must now report data security breaches to the FDPIC if there is a high risk of adverse effects on the privacy or fundamental rights of data subjects. The FDPIC should be notified of such breaches as soon as possible. Controllers should have previously drawn up a prediction of the potential implications of the breach and carried out an initial assessment as to whether there could be an imminent danger, whether data subjects need to be notified and how this could be done.

Right to data portability

The right to data disclosure and transmission under Art. 28 revFADP means that a data subject now has the option of receiving the personal data that they have provided to a private controller in a commonly used and machine-readable format, or having it transmitted to a third party. This right can be exercised free of charge, except where disclosure or transmission are associated with disproportionate cost or effort.

Enhanced supervisory powers

Under the revised FADP, the FDPIC will in future have to automatically investigate all violations; he will have the power to issue decisions in cases of poor data processing practices and must be consulted in certain cases. The new FADP sets out fines of up to CHF 250,000.

Investigation of all violations of data protection regulations

In future, the FDPIC will be required to automatically investigate all violations of the new FADP by federal bodies or individuals (Art. 49 para.1 revFADP). Under the current FADP, the FDPIC may only investigate private cases (including case investigations) on his own initiative where the processing methods used have the potential to breach the privacy of large numbers of persons. This restriction (considered a "system error") will no longer exist in future. However, as is the case under the current law, an investigation will not need to be opened for minor breaches of data protection rules (Art. 49 para. 2 revFADP). As is currently the case, the FDPIC will also be able to dispense with formal steps if initial contact with the data controller reveals that the deficiency identified was recognised and rectified in a timely manner. Owing to his limited resources, it can generally be assumed that in handling reports even after the new Act has entered into force, the FDPIC will prioritise according to the principle of discretionary prosecution.

Decisions

Under Art. 51 para. 1 revFADP, the FDPIC may now conduct proceedings according to the Administrative Procedure Act and formally rule against federal bodies or private data controllers, requiring that they modify their data processing practices in full or in part, suspend or even discontinue data processing, or delete personal data or have it destroyed. For example, the FDPIC can rule that a business must notify data subjects of a reported data security

breach. Up until now, the FDPIC only had the authority to make recommendations and, if these were not complied with, to refer the matter to the Federal Administrative Court.

Consultations

The FDPIC is neither an authorising authority nor an approval body for applications, products, regulations or projects. However, the new legislation sets out in various places that data controllers must consult the FDPIC before concluding work in these areas and implementing their projects. For example, codes of conduct and – where there are significant residual risks – data protection impact assessments must be submitted to the FDPIC for an opinion.

Unprompted opinions and information for the public

Aside from the opinions published as part of formal consultation procedures, the FDPIC is still free to express unprompted opinions on new technologies, digitalisation phenomena and the processing practices of certain sectors, and to publish his opinions and assessments. In cases of general interest, the FDPIC will also inform the public – as is the case under current law – of his observations and measures (this also applies to formal investigations).

Fees

Art. 59 revFADP regulates the services for which the FDPIC will in future charge fees to individuals. Fees will be charged for opinions on codes of conduct and on data protection impact assessments, and for approval of standard data protection clauses and binding corporate data protection rules. The FDPIC will also charge individuals fees for general consulting services in future.

Penalties

The new FADP sets out fines for individuals of up to CHF 250,000 (Art. 60 revFADP). Only intentional acts or omissions are punishable, not cases of negligence. Violation of duties to provide information and to report, and breach of due diligence and professional confidentiality are only punishable on complaint. However, failure to comply with FDPIC decisions is prosecuted ex officio. In principle, the responsible natural person is fined. However, companies can now also be fined up to CHF 50,000 if an investigation to determine the punishable natural person within the company or organisation would entail disproportionate effort.

The FDPIC is not granted powers to impose penalties under the new legislation. The offending persons are fined by the cantonal prosecution authorities. While the FDPIC can report an offence and enforce the rights of a private claimant in proceedings (Art. 65 para. 2 revFADP), he does not have the right to file a complaint.

A long process

In its 2020 autumn session, the Swiss Parliament passed the fully revised Federal Data Protection Act (FADP) as well as other amended pieces of legislation on data protection. The Federal Council is expected to bring the Act into force along with the corresponding implementing ordinances in the second half of 2022.

Background

The first Federal Act of 19 June 1992 on Data Protection entered into force in mid-1993. Following a partial revision in 2008 that sought to better inform the public about how their data was processed, it quickly became clear that rapid technological developments necessitated further amendments. In order to guarantee appropriate data protection to the public, whose daily lives are shaped by cloud computing, big data and social media, a comprehensive overhaul of the FADP was inevitable.

In autumn 2017, the Federal Council approved a draft total revision of the FADP, which it submitted to the Swiss Parliament.

Objectives of the revision

Besides strengthening the rights of data subjects, in its dispatch the Federal Council highlighted the "risk-based" approach as a guideline for the revision, according to which, the State and businesses should ascertain the risks to privacy and informational self-determination early on and incorporate the requirements of data protection at the planning stage of their digital projects. Major risks and the organisational and technical measures taken to mitigate or eliminate them should be documented. The revised FADP also promotes self-regulation, whereby members of sectors that issue a binding code of conduct are exonerated from certain obligations. The revised FADP also seeks to reinforce the FDPIC's supervisory powers.

Phased consultation

In early 2018, Parliament decided to split the revision into two parts: In order to comply with treaty implementation deadlines, initially the provisions on the processing of data were amended for federal bodies such as fedpol. This work flowed into the Schengen Data Protection Act (SDPA), which came into force on 1 March 2019 (see 27th Annual Report, Section 1.2).

The total revision of the FADP as a whole then took place in a subsequent step. In the 2019 autumn session, the National Council was the first chamber to adopt the total revision of the whole act, which Parliament then approved on 25 September 2020 once all differences had been resolved. When revising the FADP, the Federal Council and Parliament took account of the protocol amending the Convention of the Council of Europe 108[1] that had been signed by Switzerland, and the General Data Protection Regulation of the European Union (GDPR) [2]. Owing to its extraterritorial scope, the latter has already been applied by large parts of the Swiss economy since it entered into force in May 2018. Despite this dependence on European law, the new FADP is in line with Switzerland's legal tradition as it features a high level of abstraction and is technology-neutral. It sets itself apart from the GDPR not only in its brevity, but also in the sometimes different terminology it uses.

In general, it is assumed that once they have updated their data protection legislation, Switzerland and the EU will mutually recognise the equivalence of their data protection levels, so that an informal exchange of personal data across national borders will continue to be possible. The update to the EU's equivalence decision relating to Switzerland that dates back to 2000 was still pending at the editorial deadline for the annual report.

[1] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981 and ratified by the Swiss Parliament on 5 June 1997. The protocol amending the Convention was approved by Parliament in summer 2020. The Federal Council will only be able to ratify it once the new FADP enters into force.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EG (General Data Protection Regulation).

1.2 Justice, Police, Security

Information requests received by the Federal Intelligence Service (FIS)

After receiving an unusually large number of information requests in 2019, which it was initially only able to handle with significant delays, the FIS took action to reduce the backlog of requests under the FDPIC's supervision.

At the end of 2019, it was reported in various media that the FIS was receiving an unusually large number of requests concerning records in its information systems. This followed, among other things, media reports on a number of cases of politicians being spied on. The Control Delegation (CDel) of both chambers investigated the matter, and the Independent Supervisory Authority for Intelligence Activities (SA-IA) examined the keeping of files on politicians in the FIS's records and process management system.

The FDPIC approached the FIS after being alerted by public complaints to the excessively long response time in its processing of information requests. The FIS told the FDPIC that it had received around ten times more information requests than usual compared with 2019, namely more than a thousand requests in just over a year. The FIS will do everything in its power to process the pending requests within a matter of weeks. Meanwhile, it has formed a working group to modify the work processes so that the large backlog of pending requests can be reduced without compromising on quality.

In June 2020, the FIS informed the FDPIC that the additional resources provided to help it reduce the backlog of pending requests had enabled it to reply promptly to the new information requests received since May 2020. It also stated that there were still around 50 older information requests pending, which were gradually being reduced.

Federal Council adopts dispatch on revision of the DNA Profiling Act

With the revision of the DNA Profiling Act, the Federal Council intends to allow the authorities to obtain more information from DNA traces during criminal investigations. The FDPIC's call for a strict legal framework has been met.

The Federal Council adopted the dispatch on the revision of the DNA Profiling Act on 4 December 2020. With the revision, the Federal Council intends to allow the authorities to obtain more information from DNA traces during criminal investigations. On 26 January 2021, following extensive consultations with no votes against, the National Council's Security Policy Committee (SiK-N) announced its willingness to discuss the proposal. In its view, this would provide the investigating authorities with an effective tool enabling them to conduct investigations more quickly and efficiently. The Committee stressed that the draft law complied with the principle of proportionality as DNA phenotyping results were only used to solve crimes carrying a maximum prison sentence of three years or more. In current custodial sentence (see Art. 10 of the Swiss Criminal Code), only a person's sex may be determined from a DNA trace in certain cases. The proposal aims to allow the authorities also

to determine an individual's likely eye, hair and skin colour, possible biogeographical origin and age. As requested by the FDPIC, the law will contain a detailed list of the traits that may be examined.

The FDPIC had expressed his opinion on the Federal Department of Justice and Police's (FDJP) draft amendment and called for a strict legal framework (for the first office consultation, see the 27th Annual Report, Section 1.2). During the consultation procedure, as previously in relation to the preliminary draft, he expressed the opinion that phenotyping and familial DNA searches should be ordered by the compulsory measures court. These are tools that are associated with serious encroachments on fundamental rights and may only be used to solve serious crimes against physical integrity, freedom or sexual integrity. He welcomes the fact that this request was considered despite initially being rejected by the FDJP.

Bill on checking of mobile phones in the asylum procedure

The legislative project launched with the parliamentary initiative 17.423 aims to grant the State Secretariat for Migration (SEM) extended powers to check mobile data carriers for the purpose of verifying identity in the asylum and removal procedure. The Commissioner had already expressed fundamental concerns on the matter early on. He welcomes the improvements made in the meantime but stands by his opposition in principle to the bill.

The parliamentary initiative 17.423 put forward by National Councillor Rutz on 17 March 2017 calls for changes to the legal framework that would allow the SEM to analyse the mobile data carriers of asylum seekers. The Political Institutions Committees of both chambers have endorsed the initiative. On this basis, changes to the Asylum Act and the Foreign Nationals and Integration Act were drafted granting the SEM extended powers to check mobile data carriers for the purpose of verifying identity in the asylum and removal procedure.

The FDPIC commented on the bill during the consultation procedure and expressed fundamental concerns (see report of 4 June 2020). He pointed out, for example, that analysing electronic data carriers was a massive invasion of privacy for many people which required an adequate formal legal basis. The FDPIC also expressed doubts as to whether the proposed measures would produce the desired result and whether the proposed rules could be implemented in compliance with fundamental rights and in accordance with the constitutional principles of equality and proportionality, especially since the administrative asylum and removal procedure – unlike criminal procedure law – offers no actual procedural safeguards in relation to the seizure and analysis of electronic data carriers. Nor should the measure lead to people indirectly being forced to carry smart devices on their person and to produce them at all times.

The authorities concerned, including the SEM in particular, have taken the criticism constructively and have largely taken the Commissioner's comments on board. For example, compulsory confiscation of electronic data carriers has been abandoned and a formal legal basis for the measure has been established. As requested by the FDPIC, the rules now expressly state that the analysis of mobile data carriers for the purpose of verifying identity is considered a subsidiary measure that must always be implemented in a proportionate manner, and that an asylum-seeker's refusal to hand over their devices for inspection may only be taken into account during the credibility assessment. The persons concerned have a right to stay and a right to information. The position of third parties whose personal data is also affected by the analysis has also been strengthened. Finally, the Commissioner welcomes the fact that his fundamental concerns about the appropriateness and effectiveness of the planned meas-

ure will be taken into account with the introduction of a mandatory evaluation.

However, it remains unclear to the Commissioner exactly how the principles of subsidiarity and proportionality should be implemented in practice. According to the explanatory report on changes to the legal basis, other methods should be used to verify identity instead of electronic data analysis where these are possible and require less effort. Therefore, essentially, in assessing the proportionality of a method, it was important to identify the evaluation method requiring the least effort. It should be remembered that the bill allows personal data to be analysed automatically through the use of corresponding software. Subsequently, the analysis of electronic data carriers could be carried out regularly, if not routinely. However, efficiency must not be placed above the preservation of freedoms. The Commissioner must therefore stand by his opposition in principle to the bill. Beyond the context of asylum law, the Commissioner pointed out that measures restricting freedom were often initially introduced for minorities only to be gradually extended to broader segments of society in other contexts.

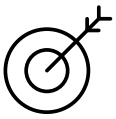
FDPIC intervenes in the Federal Customs Administration: data processing inadequately regulated in the new customs police act

The Federal Customs Administration is working on a revision of the law with a view to preparing the legal framework for the use of new digital technologies whilst providing the necessary organisational flexibility to be able to respond to changing situations in the future with even greater speed and efficiency. The Commissioner welcomes their efforts but criticises the inadequacies in the data processing rules in this large-scale project.

On 11 September 2020 the Federal Council initiated a consultation procedure on a legislative package referred to as the "act on the implementation tasks of the FOCBS", aimed at establishing the legal framework for the Federal Customs Administration's digitalisation and transformation programme (DaziT). This is a major project in financial terms involving sensitive data. The Customs Administration (including the Border Guard) is due to transition to become a new customs police office, namely the Federal Office for Customs and Border Security (FOCBS). All staff will have police powers and therefore coercive powers to collect data.

The FDPIC pointed out, in vain, to the Federal Customs Administration during the second office consultation (regarding the first office consultation, see 27th Annual Report, Section 2.4), which took place between 5 and 25 March 2020, that, in his view, the envisaged provisions on personal data processing contained serious shortcomings. In particular, they failed to grant the public the option, as required by the Federal Act on Data Protection, to assess the State's data processing activities that intruded on the public's privacy and on their right to self-determination, as well as the protection rights available to them.

The FDPIC has advised the Federal Council that government and parliament, as political bodies of the Confederation, reserve the right to regulate the basics of the data processing activities to be carried out by a single customs police system as well as the system interfaces.



Based on these considerations, the Federal Council has instructed the Administration to revise the data processing provisions, as mentioned in the consultation documents. The FDPIC welcomes the decision and is working closely with the Federal Customs Administration and the Federal Office of Justice to rectify the shortcomings identified based on practical suggestions.

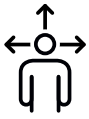
1.3 Taxation and Finance

The FDPIC advocates the right to information in international tax-related administrative assistance before the Federal Supreme Court

In 2019 the Federal Administrative Court upheld an objection by the FDPIC concerning the right to information in international tax-related administrative assistance. In the appeal procedure that followed before the Federal Supreme Court, the Commissioner again advocated the right to information. The Federal Supreme Court has yet to rule on the matter.

In international tax-related administrative assistance, the right to be informed of ongoing administrative assistance proceedings is linked to a person's right to appeal (see Art. 14 Tax Administrative Assistance Act). At the end of December 2017, the FDPIC issued a formal recommendation that, in matters of international tax-related administrative assistance, the Federal Tax Administration (FTA) should also inform in advance persons not affected (i.e. third parties) whose names are to be transmitted to the foreign authority in unredacted form (see 25th Annual Report, Section 1.9.2). This was based on the FDPIC's opinion that third parties were entitled to oppose the unlawful transmission of their data by submitting a complaint. The FTA rejected this recommendation, whereupon the FDPIC submitted the matter to the Federal Department of Finance (FDF) and then filed a complaint with the Federal Administrative Court against the FDF's negative decision (see 26th Annual Report, Section 1.3).

In its ruling of 3 September 2019, the Federal Administrative Court concluded that, in matters of international tax-related administrative assistance, persons not affected by administrative assistance requests (third parties) whose data was to be transmitted in unredacted form must, in principle, be informed in advance. The Federal Administrative Court stated that exceptional arrangements were to be made for cases requiring disproportionate effort in order to provide the necessary information, as a result of which the provision of administrative assistance would be rendered impossible or excessively delayed. The FDPIC welcomed the ruling as it protected the fundamental rights of bank staff and other third parties.



The FTA lodged an appeal with the Federal Supreme Court. The Federal Supreme Court lifted the suspension of proceedings requested by the FTA after issuing a landmark ruling (BGE 146 I 172) on 13 July 2020 on another matter concerning a similar issue. In that ruling, the Federal Supreme Court severely restricted the right to information: it stated that third parties whose data was to be transmitted in unredacted form by the FTA to the requesting foreign authority were entitled to object by lodging an appeal only in specific exceptional circumstances. Furthermore, the FTA was not required to inform all third parties entitled to lodge an appeal in advance ex officio about the transfer of data but only those persons whose entitlement to lodge an appeal was obvious based on the documents at hand.

In light of this recent ruling, the FDPIC recognised before the Federal Supreme Court that, in matters of international tax-related administrative assistance, third parties were not entitled to lodge an appeal as a rule but only by way of exception. However, the FDPIC maintained the view, confirmed by the Federal Administrative Court, that in principle all third parties should be informed in advance ex officio about the transfer of their data. Only then can all third parties who are entitled to appeal in accordance with the Federal Supreme Court ruling exercise such right and oppose an imminent transfer of their data. In addition, the FDPIC outlined again before the Federal Supreme Court how the FTA could fulfil its duty to inform without requiring a disproportionate effort that would render impossible or excessively delay the provision of international tax-related administrative assistance. The Federal Supreme Court has yet to rule on the matter.


Restaurants

1.4 Commerce and economy

Investigations into the implementation of 5G by Sunrise and Swisscom

The FDPIC has completed two independently conducted formal investigations at Sunrise and Swisscom into the implementation of the next generation (5G) telecommunication standard. Both providers pointed out that data protection and technical security were top priorities for them.

According to the technical specifications, the new 5G telecommunication standard offers enhanced security as well as higher data speeds (data transfer rates). Given the scope and topicality of the switch to 5G, the FDPIC opened two formal case investigations at Swisscom and Sunrise in 2019, when the providers were planning to introduce 5G. Both providers gave the FDPIC an insight into the concept and the progress to date in implementation and provided extensive documentation. The Commissioner was interested in a number of technical issues including the following in particular: Firstly, in 2018 a number of media reports had identified various potential vulnerabilities and known security issues in the implementation of the 5G standard. Secondly, there were security concerns regarding the suppliers used, particularly Huawei. Therefore, the FDPIC asked the companies inspected to comment on how they were addressing the known vulnerabilities and whether they depended on any individual suppliers, in particular Huawei, to an extent that could potentially compromise availability (e.g. as a result of US trade sanctions), confidentiality or data security.

Sunrise pointed out that it held regular discussions with international bodies and working groups in the telecommunications industry and that implementation was scrutinised by an independent external firm. In particular, the FDPIC considers the company's improvement measures highly valuable with a view to achieving the required level of security and an adequate level of data protection. Therefore, he recommended that Sunrise implement all the measures in question. With regard to its 5G partner and supplier Huawei, Sunrise has carried out risk analyses. These have identified risks in relation to availability, collaboration and espionage. Sunrise has defined and implemented measures to counter these provider-specific risks.

As with Sunrise, the FDPIC found no evidence to suggest any inadequacies in Swisscom's implementation in terms of data security and data protection. With regard to the issue of data security in 5G networks, Swisscom has performed internal security assessments. Like Sunrise, Swisscom also holds discussions with various international committees and working groups and follows their proven approaches to ensure the safe operation of its networks. Swisscom named its long-standing partner Ericsson as its main 5G technology supplier and explained that the components supplied by Huawei and used in antenna construction were merely passive devices, i.e. devices containing no electronic components, and were only used for sending and receiving wave signals.

The FDPIC concludes that the companies inspected have adequately addressed the issue of data security and that they consider data protection a top priority in implementation. The new 5G standard offers clear advantages over 4G in terms of enhanced information security.

Incorrect database entries at debt collection firm

The FDPIC continued his investigation into possible incorrect database entries at a leading debt collection firm and expanded the scope of the investigation.

In February 2020, the Commissioner launched an investigation into alleged incorrect database entries at a debt collection firm and thus resulting cases of mistaken identity between people with the same or similar names or addresses and possible difficulties in correcting the entries in question (see 27th Annual Report, Section 1.4). In the year under review, enquiries from members of the public and the media raised privacy issues in the designation of "negative credit-score households", too.

As a result, the FDPIC decided to expand the scope of the current investigation to include this issue. Negative household credit scores are attributed when, as part of a credit check, negative credit information is disclosed about other members of the household. For example, people with an impeccable credit score can sometimes be refused the option of paying by invoice for online orders if they live in the same household as a person with a negative credit score. The legal aspects of this matter were still being clarified at the end of the reporting year.

Car leasing credit checks

Customers planning to enter into a leasing agreement are required to give the leasing company permission to perform a credit check. To this end, the latter may collect information from third parties. The FDPIC has opened an investigation into this data processing practice.

Before a consumer may enter into a car leasing agreement, the leasing company must first check the consumer's capacity to enter into a credit agreement. To this end it needs to collect certain information on the prospective lessee to gain an understanding of the person's financial situation. If a person is found to have a negative credit history, their lease application is rejected, as set out in the Consumer Credit Act, the aim being to prevent consumers from becoming overindebted. Data processing in this context is subject to the provisions of the FADP and must not unlawfully breach the privacy of the lessee or of any third party. In particular, only the information required in order to determine a person's capacity to enter into a credit agreement may be processed.

Enquiries from members of the public alerted the FDPIC to a leasing company that required lease applicants to give their consent to collect a range of information from third parties for the purpose of checking their solvency. Applicants were also required to consent to information being collected about third parties such as spouses or family members. The FDPIC questioned whether the company's data processing practices were within the bounds of data protection law and whether the data subjects were aware of their data being processed. Therefore, the Commissioner asked the leasing company to comment on various aspects. Based on the answers given, he will decide whether to investigate further and, if necessary, recommend action to be taken.

Case investigation into Migros' video surveillance system

During the year under review, the FDPIC reviewed and evaluated Migros' new video surveillance system as part of a case investigation. Migros stated that its cameras were not used for facial recognition, automated behaviour pattern analysis or similar purposes. The FDPIC did not issue any recommendations but demanded an improvement in terms of informing customers about the system in place.

Video surveillance systems can help companies to defend their legitimate interests, for example to protect their property. However, there is growing public unease about such projects, not least because of the new technical capabilities these offer in terms of identification and analysis.

Migros' new system was among those criticised in the press and was causing some uncertainty. In his supervisory role, in order to gain a clear picture of the functions of Migros' new video surveillance system, the FDPIC requested documentation and a description of the system and the measures taken by the company to protect privacy.

After evaluating Migros' statement and the documents submitted, the FDPIC was able to determine that the new video surveillance system was limited to responsive functions: In a specific case of suspicion, the security officer of a Migros store could capture certain parameters of a suspect such as sex, height and hair colour by manually selecting a still image. The system would then search the video recordings taken in a given time frame for the same combination of parameters, and the images would be shown to security staff at the Migros store in question to help identify criminal activity.

Migros stated that its cameras were not used for facial recognition, automated behaviour pattern analysis or similar purposes. The identification of persons recorded by the video surveillance system outside the system was permitted only in specific justified cases and was subject to a procedure set out by the company.

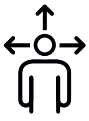
As the new video surveillance system with its limited functions does not differ significantly from the previous systems used, the FDPIC did not need to make any privacy recommendations. Furthermore, the technical and organisational measures and processes described by Migros appear adequate to ensure the security of the personal data processed in connection with the video surveillance system.

However, the FDPIC demanded improvements in terms of providing information on the new system both on Migros' website and in its privacy policy as the existing information was too general and did not explain the new system and its functions. In addition, he demanded that Migros inform him in advance and in a timely manner of any future plans, including plans to expand the functions of the video surveillance system. Migros had yet to respond at the time of the editorial deadline.

Processing of customer data by online stores

We opened an investigation into an online store to check whether its customer data processing practices complied with data protection law. We also looked into the possibility that data was being processed without users' explicit consent.

Be it because of stores closing during lockdown or the risks associated with going into stores, the coronavirus pandemic has led many people to do their shopping online. For some people, online shopping has become the only way to obtain certain goods.



Enquiries from members of the public alerted us to one of Switzerland's largest online retailers requiring customers to create a customer account and agree to all data processing activities set out in its privacy policy before allowing them to place an order.

Among other things, this meant that customers were required to consent to the recording and analysis of their purchasing behaviour in individualised, personalised form, linking to further personal data (e.g. personal data publicly available or previously collected by the company in question, by other companies within the group or by third parties), and the transfer of personal data to other companies within the group. Objections submitted to customer service were ineffective in preventing the data from being processed. The operator of the online store rejected the objections on the grounds that its privacy policy applied to all customers equally without exception and that its data processing activities were not customer options.

In spring 2020, we wrote to the operator of the online store to carry out a preliminary investigation in order to gain an overview of its data processing methods and to clarify the options available to customers to exercise their right to object. After evaluating the operator's response, we opened a case investigation. As well as assessing the data processing practices of the operator of the online store and of other companies within the group to verify their compliance with data protection law, we looked at whether data was being processed without users' express consent.

Use of Ricardo data within the TX Group

In the procedure underway, the FDPIC conducted a legal review of the use within the TX Group of personal data collected on the online auction platform ricardo.ch. We concluded that data processing carried out by the Group for the purpose of targeted marketing required users' consent. Furthermore, in our opinion, the information currently provided to users is inadequate and the privacy policy needs to be improved.

In March 2020 we concluded our fact-finding procedure opened at Ricardo and extended to the Tamedia/TX Group concerning the use within the TX Group of personal data collected on the online auction platform ricardo.ch (see our previous annual reports). The procedure focused, in particular, on ricardo.ch's new standard data privacy policy used by all TX Group companies and on the replies received from Ricardo and the TX Group regarding their data processing activities. In our final report, we carried out a legal assessment from the perspective of the Federal Act on Data Protection (FADP).

According to the Tamedia/TX Group's privacy policy, introduced for ricardo.ch in July 2017 and updated several times since then, personal data collected on the ricardo.ch platform may be transferred to TX Group companies or their partners and processed for personalisation and marketing purposes. Users' online behaviour may be monitored and evaluated using analysis tools. This data processing reportedly relies primarily on pseudonymised or anonymised data. The

data is processed for the purposes of sending or displaying on the TX Group portals anonymous advertising and of improving the security of the portals.

During our fact-finding activities, we found that the TX Group (formerly Tamedia AG) processed and analysed certain user data from the ricardo.ch platform for marketing purposes. The data collected on the various portals of the TX Group was used in aggregate form to enhance the Group's database. The Group analysed and combined data from various sources for the purpose of sending targeted advertising to users of TX Group services or to their partners through segmentation based on socio-demographic attributes (derived from the data provided by users upon registration) and presumed interests (deduced from users' online behaviour on the TX Group's portals and other partner websites). The TX Group is able to combine data via pseudonymous identifiers, mostly generated from email addresses.

We conducted a legal review of the facts of the situation. Below are some of our findings:

- The processing of data, in particular the combining of data by the TX Group and the segmentation of users, constitutes personal data processing and, as such, is subject to the Federal Data Protection Act (FADP). Furthermore, all the data collected through profiling may constitute a personality profile within the meaning of the FADP and is subject to stricter legal data protection requirements.
- In our view, such profiling for the purpose of targeted advertising requires the data subjects' explicit consent. Therefore, even if the TX Group can claim legitimate interests, these do not outweigh the right to informational self-determination of users of the ricardo.ch platform.
- Ricardo and the TX Group's data privacy policy and communication on the subject need to be improved in accordance with the principle of transparency. In particular, users must be informed in unambiguous terms as to how their data is processed by both Ricardo and the TX Group and for what purposes and whether or not they may object. If users have a right to object, they must be able to exercise it.

The FDPIC is currently assessing the next steps.

Revision of the energy ordinance

As part of the revision of the Electricity Supply Ordinance (ESO), in the interests of data subjects, the FDPIC called for a maximum retention period of two years for metering data collected by network operators. The Federal Department of the Environment, Transport, Energy and Communications (DETEC) rejected his request, referring, among other things, to the existing five-year periods in the ESO. The difference was pointed out.

In an office consultation on the revision of the Energy Ordinance, the FDPIC said that he considered the five-year retention period for load profiles specified in the ordinance to be disproportionately long. He commented that data retention of this sort affected electricity consumers throughout Switzerland. Load profiles need to be retained for five years for the purpose of optimising power consumption although it is reasonable to assume that the majority of data subjects will never analyse this data. Milder means are also available for the purposes of balance network management and billing to achieve the desired objectives, for example aggregation based on tariff type (e.g. high vs. low tariffs) for billing, whereby load profiles would no longer be needed for billing purposes. In accordance with the ESO, personal data and personality profiles are destroyed after twelve months providing, they are not needed for billing purposes or anonymised.

An extended retention period of five years is problematic particularly because load profiles constitute personality profiles and, under the revised FADP, amount to profiling, which is subject to stricter data protection requirements.

Therefore, the FDPIC takes the view that personal data should be deleted after twelve months or else, for practical reasons, after two years at the latest if the data subject has not given explicit consent for the data to be kept for longer, for example in order to receive information about their load profile for the purpose of evaluating solutions designed to increase energy efficiency. The provision in question should be amended to maintain the existing twelve-month retention period for load profiles, allowing it to be extended to a maximum of five years with the customer's explicit consent.

1.5 Health

Requirements for cloud services used to process patient data

Cloud services are increasingly being used in the healthcare sector in the processing of patient data. In his advisory role, the FDPIC has pointed out a number of aspects that healthcare professionals need to consider when choosing a cloud service provider.

During the year under review, the FDPIC was regularly contacted by physicians, psychologists and other healthcare professionals regarding the use of cloud services for patient data processing. Their enquiries concerned the processing and storage of health data at data centres operated by external providers ("cloud providers"), specifically storage, transfer and destruction of patient records, for example when a patient dies or a medical practice closes.

In its advisory role, the FDPIC pointed out that physicians were also responsible for ensuring data security when using cloud services even though they had limited control over data security when using such services. Therefore, physicians had to choose their cloud provider carefully, bearing in mind the following requirements:

- Data should remain in Switzerland;
- The contract with the cloud provider should meet the requirements of patient confidentiality;
- All persons with access to patient information are bound to maintain patient confidentiality;
- It should be possible to delete patient information at any time;
- It should be possible to request a list of all persons with access to the information at any time;
- Data security should be checked regularly and the audits made available;
- The physician should be given the details of a contact person for matters relating to data protection;
- Daily backups should be possible;
- All connections must be encrypted and two-factor authentication must be available to protect data from unauthorised access.

In conclusion, therefore, the FDPIC advises against the use of popular free cloud services for sharing or storing patient data as these typically fail to meet the requirements outlined above.

CORONA

Case investigation at myvaccines.ch

The electronic vaccination platform myvaccines.ch was launched by a foundation years before the pandemic struck. The platform was financially supported by the Federal Office of Public Health (FOPH) among others and designed as an electronic alternative to the standard vaccination record.

During the COVID-19 pandemic, the number of people using the platform increased significantly, partly in connection with the interfaces to the application promoted by the FOPH for the registration of people seeking vaccination. The foundation also developed and operated a specific module for documenting COVID-19 vaccinations (myCOVIDvac) on behalf of the FOPH.

At the end of March 2021, the Commissioner was confronted with the results of a journalistic investigation which pointed to possible serious security and data protection flaws on the myvaccines.ch platform. After consultation with the National Cyber Security Centre (NCSC), the Commissioner launched a formal investigation within a day and recommended that the foundation cease operations immediately. At the end of the financial year, the procedure was still ongoing and there was no information as to when the platform might resume operation.

Furthermore, in consultation with the cantonal data protection authorities, the FDPIC has worked to ensure that other platforms operated by private individuals on behalf of the federal and cantonal health authorities, or recommended by the same, in the fight against the pandemic are examined more closely.

CORONA

Data protection challenges of introducing facilitations for people who have been vaccinated

The availability of COVID-19 vaccines has sparked a public debate on the lifting of bans and restrictions on personal freedom for people who have been vaccinated. Since December 2020, the FDPIC has publicly stated that the processing of health data by the State and the private sector required in order to offer facilitations to people who have been vaccinated should be carried out in accordance with clear public law requirements and should not mean that everyone is required to carry a smartphone.

With the prospect of vaccination against the COVID-19 virus on the horizon, the second wave of the pandemic has sparked a public debate on the lifting of bans and restrictions on personal freedom for people who have been vaccinated. The Political Institutions Committees of both chambers discussed how this could be implemented from a legal point of view in consultation with the Commissioner (see PIC-S media release of 23.02.2021).

The State and private individuals who perform state functions may provide differential treatment based on Covid vaccination status only if there is a corresponding statutory basis. By contrast, private individuals may, in principle, provide differential treatment without an explicit legal basis in accordance with the freedom of contract.

If private individuals make access to goods or services conditional on customers or guests being vaccinated, they will be regularly processing the health data of their fellow citizens, which can potentially lead to violations of privacy. Therefore, at the beginning of the public debate and in the hearings mentioned above, the Commissioner took the view that legal requirements needed to be set for this scenario. He also pointed out the data protection requirements that private individuals need to ensure are met if they wish to make access to goods or services conditional on a negative test result or proof of vaccination (see our news briefing of 22.01.2021).

Therefore, the collection and processing of personal data must be proportionate and necessary for the intended purpose, namely protecting people from infection and preventing the spread of the disease. Furthermore, access to goods or services should not be made conditional on the provision of health data in cases where data subjects cannot reasonably be expected to forego the goods or services in question. Finally, with regard to the processing method, the FDPIC pointed out that people who are unable or unwilling to show proof of vaccination on a smartphone must be offered reasonable alternatives to the digital processing of the personal data mentioned in comparable conditions.

This last aspect is particularly important to the Commissioner as it may be assumed that the systematic processing of personal data by private individuals in connection with the pandemic will shape the informational self-determination of people beyond the current crisis.

CORONA

Implementation of a data protection-compliant COVID-19 certificate

As people will be required to prove that they have been vaccinated against COVID-19, that they have recovered from the disease or that they have tested negative before they are allowed to travel abroad, in March 2021 the Swiss Parliament established a legal provision for the introduction of a standardised, forgery-proof, internationally recognised COVID-19 vaccination certificate. The Commissioner is monitoring the implementation work of the Federal Office of Public Health (FOPH) as part of his advisory duties as a statutory supervisory body.

During the second wave of the pandemic, we saw the need for a reliable solution allowing people who had been vaccinated, had recovered or had tested negative for the coronavirus to provide the corresponding proof, initially for international travel but possibly also for other purposes. Up until then, Switzerland did not have any specific legal regulations governing the form and content of a vaccination certificate. Proof of COVID-19 vaccination and test results were also provided in paper form, by SMS or email or as a verifiable entry on a relevant platform. However, the various options available did not all meet the requirements of data protection law, which prompted the FDPIC to intervene in his capacity as the supervisory authority (see box "myvaccines.ch").

In March 2021, the federal legislators introduced a standardised, internationally recognised COVID-19 vaccination certificate with the new Article 6a of the COVID-19 Act. The provision sets out the requirements for vaccination, test and recovery certificates: The certificates must be personalised, forgery-proof, verifiable while complying with data protection requirements, and designed so as to allow only decentralised or local verification of their authenticity and validity. It should also be possible for the certificates to be used when entering or leaving other countries. The legislators' requirement that the certificate be made available on paper in future as well as digitally also reflects the Commissioner's demand that the use of electronic certificates should not mean that everyone is required to carry a smartphone.

Furthermore, the provision states that the Confederation may provide the cantons and third parties with a system for issuing certificates. On 29 March 2021, the FOPH set up a project group in order to develop such a system. The FDPIC is advising the group in his capacity as the supervisory authority. His demands in terms of compliance with data protection requirements largely coincide with the position of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on the Digital Green Certificate, which is to be introduced in the EU for international travel. In addition, the FDPIC has drawn up data protection requirements for the project group in terms of a data-minimising design for the certificates for possible further uses in Switzerland. The Commissioner calls for the creation of a basis under public law to regulate further uses of the certificates by the authorities and private individuals (see text above).

Electronic patient records: First reference communities certified

Electronic patient records (EPRs) are about to be launched across Switzerland. The FDPIC followed the development of the certification processes. He then established contact with new reference communities and stepped up discussions with existing contacts. Meanwhile, the first reference communities have been certified.

Electronic patient records (EPRs) are a virtual collection of links allowing individuals to access their personal health data, for example medical reports or prescriptions, in digital format. These records contain sensitive personal data, which may only be processed with the explicit consent of the data subjects. Patients must be provided with comprehensive and complete information in this regard. The FDPIC emphasised the importance of handling this matter properly. During the year under review, he inspected various reference community documents.

Brought into force on 15 April 2017, the Federal Act on the Electronic Patient Record (EPRA) allows patients to manage all access rights for each individual document themselves. This involves properly setting data privacy levels for each document, assigning user roles for individual health professionals, setting rules for proxies and specifying that, in an emergency, access should only be granted with the prior authorisation of the healthcare professional treating the patient. The FDPIC examined these aspects, too, and will continue to monitor the controlling of access rights, in particular after completion of the certification processes for reference communities, so that patients may retain control over their data, even after they have given their consent. The FDPIC continues to liaise with the FOPH, the providers of the technical infrastructure and the cantonal data protection authorities. Among other things, this contact is important in clarifying responsibilities given that certain healthcare providers such as hospitals are subject to supervision by the cantonal data protection authorities whereas physicians and reference communities are subject to supervision by the FDPIC.

Reference communities were due to become operational in April 2020. However, the planned launch date was delayed after the certification processes took longer than anticipated. In mid-November 2020, eHealth Aargau (SteHAG) was the first reference community to be certified under the EPRA. In late December 2020, the eSANITA association's reference community in south-eastern Switzerland was the second EPR provider to complete the certification process. The FDPIC asked both communities to outline the main data protection risks they had identified to date in connection with EPRs, the measures in place to counter these risks and the way in which they fulfil their data protection responsibilities in this respect.

The FDPIC's key contacts will be the data protection and data security officers, whom the reference communities are required to appoint under the EPRO.

CORONA

Swiss proximity tracing app (SwissCovid app)

Early on in the coronavirus pandemic, the FDPIC was approached by the developers of a proximity tracing system, which went on to become the SwissCovid app, for advisory support in their work. The system uses Bluetooth technology to identify epidemiologically relevant contacts between mobile phones and logs them locally. The FDPIC closely monitored the development of the SwissCovid app, initially from a technical point of view and later on also from a legislative perspective.

On 21 March 2020, just a few days after Switzerland declared an "extraordinary situation" under the Epidemics Act (EpidA), the FDPIC was contacted by the developers of a Covid proximity tracing app for a data protection assessment. Project managers at the Federal Institute of Technology Lausanne (EPFL) and in the private sector were working on the development an application that would alert people who had installed the Covid app on their smartphones if they had recently come into contact with someone with the same app installed on their own device who had later tested positive for the coronavirus. In his initial assessment, the FDPIC found that the project had addressed important concerns regarding the protection of privacy and informational self-determination by not collecting location data, using temporary identification codes and making participation voluntary.

The EPFL and its partners went on to develop what became known as the Decentralised Privacy-Preserving Proximity Tracing (DP-3T) app. Their work was carried out independently of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project and featured improvements in terms of privacy with its decentralised approach to data processing. We welcomed the fact that the central server essential even with a decentralised approach would only receive anonymous keys and that epidemiologically relevant contacts would only be stored locally on the smartphones themselves.

Later on in the project, the Confederation decided to introduce an official contact-tracing system based on the DP-3T. From then on, the Federal Office of Public Health (FOPH) – the authority responsible for operating the system – involved us in the implementation work on what would become the SwissCovid app and provided us with comprehensive documentation. This enabled our specialists to conduct a technical review of the app and its system architecture, including implementation of the backend server. In May, based on a data protection impact assessment among other things, the FDPIC found that the system met the data protection requirements for a pilot trial to begin (see the FDPIC's opinion of 13 May 2020).

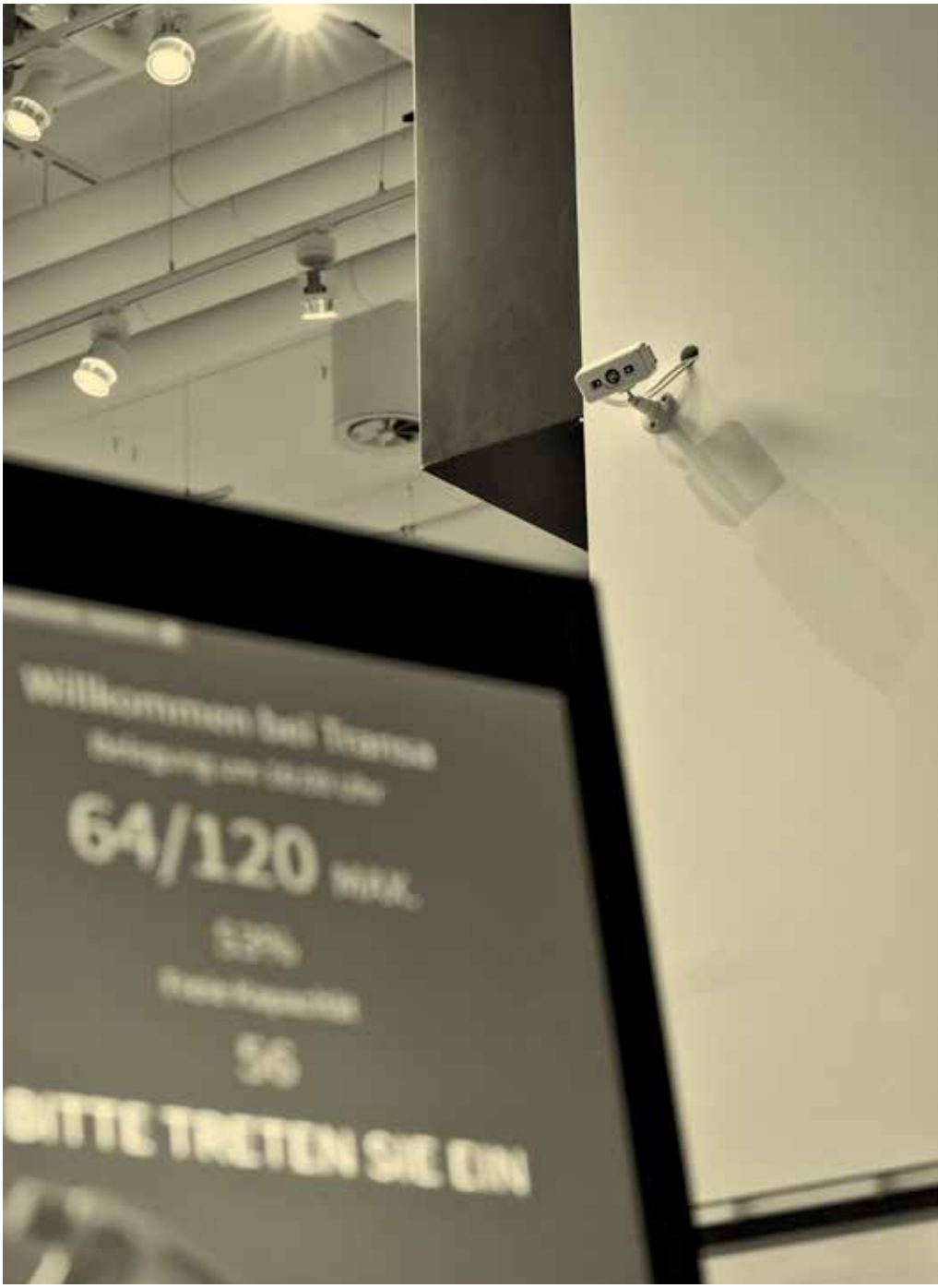
After reviewing a report published by the National Cyber Security Centre (NCSC) in June, the FDPIC confirmed his assessment. He emphasised that the use of the Google and Apple application programming interfaces (APIs) – widely criticised in data protection circles and media reports – for the SwissCovid app did not represent a significantly greater risk compared to other everyday uses that the public made of these interfaces.

The Commissioner called on the Federal Administration to initiate the development of a specific legal basis for the app in the Epidemics Act in accordance with Article 17 FADP but his request was turned down. Subsequently, however, he was able to advise the competent parliamentary committees to develop such a basis. This was enshrined in the law with the urgent introduction of a new Article 60a in the Epidemics Act on 25 June 2020.

According to this provision, use of the SwissCovid app is voluntary. On the one hand, the legislator was aware that obliging people to use the app would be difficult to explain politically and hard to implement given that the Bluetooth function could be deactivated at any time; on the other hand, Parliament sent

a signal that it was against obliging individuals to carry a smartphone on them by prohibiting authorities, companies and individuals from favouring or penalising anyone based on whether or not they used the app.

On 25 June 2020, the Swiss-Covid app was launched in Apple and Google app stores. While some people still have serious privacy concerns months after its launch, others accuse the legislator of excessively restricting the app's effectiveness by favouring privacy. Faced with these conflicting attitudes, the FOPH has not yet succeeded in increasing distribution of the app beyond the impressive figures of around three million downloads and 1.7 million active users, thus falling short of its optimistic expectations.



CORONA

The legal framework for collecting contact details

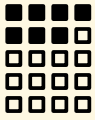
As a result of the FDPIC's intervention, an adequately defined legal framework has been established for the collection of contact details for the purpose of Covid-19 contact tracing in compliance with the provisions of the Federal Act on Data Protection.

When restaurants, bars, clubs, fitness centres and other public establishments reopened on 11 May 2020, many planned to collect contact details for the purpose of tracing potentially infected persons as part of the Covid protection plan ordered by the Federal Council. As there was initially no legal framework in place for the collecting and processing of contact details, the FDPIC publicly announced that, for the time being, this information should be collected on a voluntary basis only (see our Communication of 19.05.2020 on Coronavirus protection plans).

As a result of the FDPIC's intervention, the Federal Council established an adequately defined legal framework for the mandatory collection of contact details introduced on 22 June 2020. In its COVID-19 Special Situation Ordinance it restricts the use of the collected data (transfer to the competent cantonal authority for the purpose of contact tracing if a person is found to be infected), sets out the requirements regarding data storage (maintenance of confidentiality) and automatic deletion after 14 days, and specifies the categories of data to be collected at federal level (surname, first name, address and telephone number).

In order to improve the efficiency of contact tracing, some cantons have obliged restaurants and bars to use a specific app to collect contact details. The FDPIC pointing out the need for a clear (cantonal) legal basis and emphasised that the apps used needed to guarantee that data would be processed in a transparent, purpose-specific and secure way. He also drove home the point that private individuals could not oblige their customers de facto to carry a smartphone: Some people are not willing to produce a smart device with a specific programme installed for fear of their digital lifestyle data being accessed, while others are not able to do so because of their age, health condition or disability. As well as offering digital tools for collecting information, private companies must also offer alternative tools such as paper forms to fill out in specific circumstances.

Since summer 2020, a number of legal and technical problems have emerged in connection with the use of specific apps for collecting contact details. This has prompted the FDPIC to open a case investigation into an app widely used in various parts of Switzerland. The FDPIC is keen to complete the investigation before restaurants reopen, although this is a major challenge given the formalities involved in the procedure.



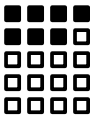
1.6 Employment

Permissibility of background checks in the application process

Swiss employers are increasingly being offered, by foreign companies in particular, the opportunity to search databases for information on job applicants and to provide recommendations for employment. The FDPIC has been contacted on numerous occasions regarding the permissibility of such background checks.

According to Article 328b of the Swiss Code of Obligations, employers may only handle data that is required for the application process. In doing so, they have a duty to observe the data processing principles set out in the FADP, in particular the principle of proportionality and the requirement for transparency.

The principle of proportionality requires that database searches and subsequent data evaluation be conducted only to the extent deemed appropriate, necessary and reasonable for the purpose of checking applicants' qualifications. More or less extensive personnel security screening may be considered appropriate, necessary and reasonable in areas in which employees have access to sensitive information with a view to minimising certain risks, for example in the banking or security sectors. However, full background checks are considered disproportionate in cases where there are no particular risks, except in special circumstances, for example in the case of teachers.



Regardless of the question of proportionality, in accordance with the transparency requirement, employers have a duty to inform the person concerned about the background check and the data processing and evaluations carried out as part of it. This is necessary in order to allow the person concerned to verify the lawfulness of data processing and the accuracy of the data collected and to assert his or her rights. In the light of the requirement for transparency background checks that are conducted in secret and thus not disclosed to the subjects are therefore unlawful.

CORONA

Data protection aspects of working from home

During the year under review, many employees were forced to work from home. As a result, the FDPIC faced a surge in enquiries regarding the use of various video conference solutions, employee monitoring and access to Swiss company servers from abroad.

The requirements that need to be met for employees to be allowed to work from home are governed by labour law. However, from a data protection point of view, this new setup raises important issues for example regarding the use of digital communication tools for audio- and videoconferences (see chapter 1.1, box to corresponding guide) and data sharing platforms. Employees' duties may change over time, but employers remain responsible for ensuring information security and data protection even in times of crisis and are therefore still required to comply with the data processing principles laid down in the FADP. In that sense, it is therefore up to employers to choose software programs that guarantee adequate protection of personal data being processed. On the FDPIC's website under the heading "Measures for the safe use of audio and video conferencing systems", you will find a guide to the key data protection requirements to be observed when choosing such platforms.

The FDPIC received many enquiries from members of the public concerned about being constantly monitored by their employers while working from home. The FDPIC is aware that, depending on the IT solution used, the behaviour of employees working from home can easily be monitored constantly although this is unlawful under the FADP and expressly prohibited by labour law.

Finally, the FDPIC was repeatedly asked whether employees working from home outside of Switzerland and accessing the company server in Switzerland from abroad – be it employees working from their holiday home abroad or cross-border commuters working from home – constituted cross-border disclosure of data. However, as long as employees working from home abroad access the company server via a Virtual Private Network (VPN) and process personal data only to the extent that they would normally do in the company workplace, and, in particular, do not provide access to the personal data to anyone abroad, in the FDPIC's view it does not constitute cross-border disclosure of data within the meaning of the FADP. Regardless of whether employees working from home do so in Switzerland or abroad, the confidentiality of personal data must be guaranteed at all times.

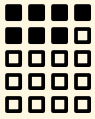
CORONA

Data protection requirements for early detection of coronavirus in the workplace

The coronavirus pandemic has raised many questions regarding compliance with data protection requirements in the employment relationship, for example relating to the legality of taking employees' temperature at work or the announcement of cases of infection within the company. Time and again, the proportionality of these measures was questioned.

During the employment relationship, the employer may only process employee data that is necessary for performance of the employment contract. The principle of proportionality laid down in the FADP must always be observed. Accordingly, any processing of personal data must be appropriate, necessary and reasonable in order to achieve the desired goal, in this case preventing the spread of infection in the workplace.

With regard to taking employees' temperature at work, the question was raised as to whether this measure was indeed a reliable way of reducing infection: On the one hand, a raised temperature can be a symptom of another disease, and on the other hand, body temperature can easily be artificially lowered by medication. Furthermore, some people infected do not go on to develop a fever. Therefore, comprehensive temperature screening is considered to have limited efficacy in preventing infection in the workplace.



Consequently, employers need to consider other less intrusive measures that serve the same purpose. In these cases, the FDPIC suggested that any employees showing symptoms typical of coronavirus should be obliged to report immediately to a trusted person within the company. The FDPIC based his assessment of the issue on the recommendations of the Swiss National COVID-19 Science Task Force, which expressly advises against temperature screening as a stand-alone preventive measure.

Another question frequently raised was that of how employers may or should inform their employees of cases of infection within the company so that colleagues who have come into contact with the infected persons can self-isolate. Employers have a duty of care towards their employees and are therefore required to process this information even though contact tracing is effectively the responsibility of the cantonal authorities (cantonal medical officer), not employers.

1.7 Insurance

Introduction of the HIS reporting and information system in the Swiss insurance business

The FDPIC advised the Swiss Insurance Association on the introduction of the HIS reporting and information system, a database for participating insurance companies designed to help combat insurance fraud. The FDPIC emphasised that all data processing in connection with the operation of the HIS system must comply with the data protection principle of proportionality.

The FDPIC's advisory activities on the HIS system began in the reporting year 2017/18 (see 25th Annual Report, sub-section 1.6.2) and are ongoing.

Swiss insurance companies that have signed up to the HIS system use it to report individuals for whom irregularities as set out in the rules – e.g. breach of disclosure obligation under Art. 6 of the Insurance Policies Act (IPA) – were identified during a claims settlement procedure. When future claims are processed and the database is searched for the individual in question, the latter will be shown as flagged in the system for having been associated with an irregularity in the past, thus prompting the insurance company to closely verify its obligation to pay in the case of any new claims. Individuals may be flagged for breaches of insurance policy or liability law but not criminal law. Insurance companies may only query whether an individual is present in the HIS database if the latter is involved in a new claim, not outside the claims management context, so not, for example, before concluding a contract with the individual in question. The HIS database contains the details of the insured person and of any other individuals involved in a claim such as "instigators" or "accomplices".

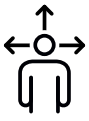
In his advisory capacity, the FDPIC emphasised, in particular, that all data processing in connection with the HIS system must comply with the data protection principle of proportionality. Accordingly, an individual may be entered in the HIS system where appropriate and necessary for the purpose of detecting and preventing insurance fraud, and the data subject can reasonably be expected to tolerate the resulting invasion of privacy. The grounds for flagging an individual must be restricted to specific circumstances that are transparent and clearly set out in the rules. Flagging is intended to prompt insurance companies to examine the insured person's payment request in detail for subsequent claims but must not be used to prejudge people. Therefore, measures must be in place to ensure that the personal data in the system is correct. It should be possible to identify and penalise insurance companies that fail to observe the rules and repeatedly make unjustified entries in the database.

Most of the FDPIC's suggestions have been implemented. In particular, the grounds for flagging an individual in the HIS system have been specified in greater detail. Only experience will show how effective the HIS system is in helping to prevent insurance fraud, how well the insurance companies are sticking to the rules and whether any improvements will be needed in the future from a data protection perspective.

Transfer of membership data to sponsors

The FDPIC demands that valid consent be obtained from data subjects before their data may be lawfully shared with sponsors. Members of associations must be allowed to object to their data being shared without being disproportionately affected as a result.

During the year under review, the FDPIC received several enquiries about the sharing of addresses of association members with sponsors for advertising purposes. He was asked whether it was permissible to charge a higher membership fee to members who had objected to their data being shared. We pointed out to the persons and associations concerned that increasing the fee to the point that the persons concerned practically felt forced to agree to their data being shared could be considered to constitute a disproportionate disadvantage.



The FDPIC had already contacted sports associations and sponsors to draw their attention to their obligations in terms of observing data protection regulations when processing data (see 22nd Annual Report 2014/15, sub-section 1.8.5). Associations may not pass on any data to sponsors without the valid consent of the data subjects. For data sharing to be considered lawful, all data subjects must be adequately informed in advance of any data sharing (i.e. what data is to be shared with whom and for what purpose) and given a chance to consent. If an opt-out approach is used, it is crucial that members be given an easy way to object to their data being shared without being disproportionately affected as a result. Sponsors, in turn, must guarantee contractually that they only process the addresses of association members that were passed on to them on the basis of valid consent.

Systematic use of the OASI number by the authorities: amendment of the law approved by Parliament

On 18 December 2020, Parliament approved an amendment to the Federal Act on Old-Age and Survivors Insurance (OASI) that lists a range of authorities, organisations and persons authorised to routinely use the 13-digit OASI number (NAVS13/AHVN13) as a unique identifier outside the context of social insurance. The Commissioner has secured important data protection guarantees.

On 1 February 2017, the Federal Council instructed the Federal Department of Home Affairs (FDHA) to carry out a consultation on the systematic use of the NAVS13 by federal, cantonal and municipal authorities. An internal working group set up within the Administration, which we had not been invited to join, deemed, at the time, that this presented no particular privacy risks. However, both the FDPIC and the cantonal data protection commissioners already opposed the principle of systematic use of the NAVS13 because of the associated privacy risks.

Therefore, together with the Federal Office of Justice (FOJ), we requested an assessment of the risks of systematic use of the OASI number, which was assigned to Prof. David Basin, a professor at the Swiss Federal Institute of Technology Zurich. In the conclusions of his assessment of 27 September 2017, Prof. Basin emphasised that the systematic use of the NAVS13 presented significant privacy risks (see 25th Annual Report, sub-section 1.1.2). The expert recommended using sector-specific identifiers. However, he also pointed out that such a measure would not have the expected results in terms of protecting data without taking other important measures such as updating the database architecture.

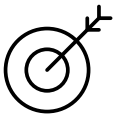
Following this report, the National Council Legal Affairs Committee submitted a postulate (17.3968) on 20 October 2017 asking the Federal Council to develop a concept of how to manage the risks associated with using the NAVS13 as a unique personal identifier. The concept also had to show how data protection could be improved in relation to the use of personal identification numbers by cantons, municipalities and third parties, with due consideration of the FDPIC's opinion. In its response of 20 December 2017, the Federal Council stated that it was aware of the potential risks associated with the use of the NAVS13 and declared that it would take on board the Basin study and the Commissioner's comments in its bill.

During the pre-consultation of the offices, we successfully requested several changes to the bill, for example introducing the requirement that all entities authorised to routinely use the NAVS13 conduct risk analyses and keep a register of the databases in which the NAVS13 is stored. Furthermore, the need to strengthen technical and organisational measures aimed at reducing the risks of data breaches was recognised and incorporated in the bill (see 27th Annual Report, Section 1.7).

On 7 November 2018, the Federal Council initiated the consultation procedure on the amendment of the OASI Act, which provides for the systematic use of the NAVS13. However, the bill took into account the Commissioner's data protection requirements. An authority may link factual data (first name, last name, date of birth etc.) to the NAVS13 and check their accuracy in the Unique Person Identification (UPI) database managed by the Central Compensation Office (CCO). However, it cannot access the other registers, namely the central register of insured persons, the register of benefits of the CCO or the registers containing factual data kept by other authorities. This prevents an authority from being able to link different databases and create personality profiles, which are generally very accurate, based on the NAVS13. Therefore, we welcome the fact that the bill obliges all federal and cantonal bodies, decen-

tralised units of the Federal Administration and organisations and persons under public or private law outside the offices with access to such databases to carry out periodic risk analyses focusing specifically on the danger of unauthorised data matching. Based on that risk analysis, state-of-the-art data protection and security measures must be developed and implemented, tailored to the specific risks involved. The entities designated in the bill that routinely use the NAVS13 are required to keep a register of the relevant databases used, in particular, as a basis for the required risk analyses. Other entities authorised by law to use the NAVS13 routinely, besides the federal, cantonal and municipal authorities, are educational establishments, private insurance companies (also within the context of supplemental insurance) and organisations and persons under public or private law, outside the above-mentioned authorities, who are entrusted with administrative tasks under federal, cantonal or municipal law or by contract, where the applicable law provides for the systematic use of the OASI number. In addition, the NAVS13 may not be used for purely private purposes. This applies even if the data subjects have consented to the systematic use of their NAVS13 by private individuals.

In addition to the measures mentioned above, we welcome the fact that the Act also sets out mandatory technical and organisational measures offering protection against possible misuse of the OASI number. For example, the Act sets out the rule that access to databases containing the NAVS13 is to be restricted to those persons who need the number to carry out their duties. In addition, files containing the NAVS13 are to be sent in encrypted form via the public data file network. Finally, authorities, organisations and persons authorised to use the OASI number must draw up a procedure to follow in the event of unauthorised access to or misuse of the databases, and their staff must be trained to use the OASI number in accordance with the law. Failure to comply with these duties is punishable by law.



No further significant amendments were made to the bill after the consultation procedure. In December 2020, just before the final vote, Parliament extended the list of entities authorised to use the NAVS13 routinely to include bodies responsible for carrying out the checks required under a legally binding collective employment agreement.

The numerous hearings of the Commissioner by the parliamentary committees during the legislative process have made it possible to enshrine data protection in law. The new regulations are due to come into force no sooner than the end of 2021.

1.8 Traffic and transport

Surge in enquiries from the public regarding drones

During the year under review there was a surge in enquiries from members of the public regarding drones. Enquiries were received from drone owners as well as persons feeling uneasy about drones taking pictures or videos.
It seems that drones are becoming increasingly popular with private individuals. At least, the FDPIC registered a sharp increase in the number of enquiries from members of the public on the subject during the year under review. Some were from people wanting to take pictures and videos using a drone and enquiring about the regulations surrounding data protection with the Commissioner and other authorities (in particular the Federal Office of Civil Aviation FOCA); others were from members of the public concerned about drones circling their homes or workplaces and possibly taking pictures or videos.

As well as seeking legal advice, those contacting the FDPIC are often seeking a decision from the Commissioner on their specific case. In such cases, the FDPIC points out that the general data protection principles are to be observed and that private data processors need a justification. For authorisations and bans he refers to the competent authorities, in particular the FOCA and the cantonal civil and criminal courts.

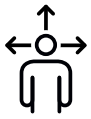
On our website you will find a fact sheet with more information on video surveillance with drones by private individuals (see Website, fact sheet not available in English).

Revision of the Passenger Transport Act: Avoiding discriminatory barriers for people travelling anonymously on public transport

The FDPIC expressed his opinion during the "Office consultation on the dispatch on the amendment of the Passenger Transport Act – a modern basis for public transport".
Since the office consultation, several meetings have taken place with representatives of the Federal Office of Transport and the Federal Office of Justice. The discussions centred, in particular on the extent to which transport companies should be obliged to comply with data protection regulations for private individuals or public authorities.

The FDPIC pointed out, in particular, that if they are made to comply with the regulations applicable to private data processors, in addition to consent, all other justifications, such as the legal basis or overriding interests, are available. Transport companies may claim an overriding interest, for example, when they process personal data directly in connection with the conclusion or performance of a contract.

Where personal data is processed based on consent, the requirements for legally valid consent must be met: Consent must be freely given on the provision of adequate, transparent information. If sensitive personal data or personality profiles are to be processed, consent must be given explicitly. Furthermore, passenger transport



may not be made conditional on consent being given to the processing of personal data for other purposes. If data is to be processed for other purposes, separate consent must be obtained for each data processing operation.

Even in cases where implicit consent is sufficient, passengers must be fully informed so that they are able to recognise invasions of personal privacy and have a real choice to opt for either offerings that are conditional on data collection or alternative anonymous offerings with comparable conditions. If they choose offerings that are conditional on data collection, this constitutes implicit consent. The FDPIC also stated that alternative anonymous offerings must not be linked to any deterrent or discriminatory financial or administrative barriers. Since passing on the additional costs associated with alternative offerings could potentially result in certain sections of the population being excluded from such offerings, the FDPIC demanded that the relevant provision of the Passenger Transport Act be amended accordingly and that justification be defined more accurately in the dispatch.

With regard to the sales infrastructure and the central ordering platform, which has yet to be implemented, the FDPIC drew attention to the general rules already applicable and the new requirements to be observed under the fully revised FADP when setting up the digital platform, such as privacy-friendly technical design and default settings ("privacy by design" and "privacy by default") and the protection of persistent data.

The FDPIC will continue monitoring the legislative process and working to ensure that the data protection requirements are taken into account.

Use of airline passenger data to combat terrorism

The Federal Department of Justice and Police (FDJP) is fleshing out a legislative project on the use of airline passenger data to combat crime and terrorism in Switzerland. The FDPIC is on the committee of external experts overseeing the project.

On 12 February 2020, the Federal Council announced that, in principle, it was in favour of using airline passenger data (passenger name records, PNR) to combat crime and terrorism in Switzerland. To this end, the FDJP was tasked with taking the first steps to introduce a national PNR system (see 27th Annual Report, Section 1.2, p. 27). The FDJP has been instructed to flesh out with the Federal Department of the Environment, Transport, Energy and Communications (DETEC) by mid 2021 a bill to be submitted for consultation for a federal act on the collection and use of PNR data by Switzerland and transmission of the same to countries whose data protection and processing practices met the standards of the EU Directive 2016/681 of 27 April 2016 on the use of airline passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (EU PNR directive). The FDJP is also to work with the Federal Department of Foreign Affairs (FDFA) to prepare a mandate by mid 2021 for negotiations with the EU for an agreement on the exchange of PNR data between the competent co-ordination offices (Passenger Information Unit, PIU) in Switzerland and EU Member States.

The FDPIC has taken up a seat on the PNR project committee of external experts and is overseeing the project to ensure compliance with data protection law. In setting up a PNR system, fundamental rights may be restricted only to the extent necessary to accomplish the intended purpose. A balance must be maintained between guaranteeing fundamental rights and imposing the restrictions needed in order to ensure public safety. This includes using the "push method" of data transfer, meaning that foreign authorities will not have direct access to the data. Furthermore, the Commissioner is keen to compile a list of crimes according to his long-standing practice. This is in line with the principle of proportionality and promotes transparency.

The Privacy Shield does not guarantee data subjects in Switzerland an adequate level of protection for data transfer to the US

Following his annual reviews and recent rulings by the Court of Justice of the European Union (CJEU), the FDPIC has reassessed the data protection conformity of the Privacy Shield regime. He concludes that the Privacy Shield regime does not provide an adequate level of protection for data subjects in Switzerland and advises Swiss companies to conduct a case-by-case assessment of the disclosure risks when transferring data to the US based on contractual guarantees.

In his evaluation reports for the 2018 and 2019 Swiss-US Privacy Shield reviews, the FDPIC pointed out that, despite improvements introduced since it came into force, the Privacy Shield regime failed to offer data subjects sufficient enforceable legal rights in the event of the US authorities' gaining access to their personal data (see also 27th Annual Report, p. 34, and 26th Annual Report, Section 1.2). In particular, he lamented the fact that the ombudsperson mechanism – which is intended to guarantee an indirectly enforceable legal remedy – could not be assessed in terms of its effectiveness owing a lack of transparency. Furthermore, it was unclear whether the ombudsperson had decision-making powers vis-à-vis the US intelligence services or was truly independent. The FDPIC considered the lack of transparency a problem, along with the resulting absence of guarantees concerning the invasion of privacy by US authorities in respect of data subjects residing in Switzerland.

On 16 July 2020 the Court of Justice of the European Union (CJEU) issued a judgement in the case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems ("Schrems II judgment") declaring invalid the Adequacy Decision 2016/1250 by the EU Commission regarding US companies certified under the Privacy Shield regime. The CJEU also clarified that the use of standard contractual clauses (SCC) for the transfer of data to the US and other third countries that did not offer adequate data protection required a case-by-case assessment of the suitability of such clauses and, if necessary, an amendment. This ruling is not binding on Switzerland. Under the GDPR, however, EU data protection law and any CJEU rulings based thereon are applied by authorities and courts in the EU and EEA also with respect to Swiss companies if the latter process data in such a way that they fall within the scope of the GDPR. After carefully examining the CJEU judgment and the Swiss legal situation, the FDPIC concluded in his opinion of 8 September 2020 (see press release) that, despite guaranteeing special protection rights for data subjects in Switzerland as well, the Privacy Shield regime did not meet the requirements of adequate data protection as defined by the FADP for the transfer of data from Switzerland to the US. In the light of this assessment based on Swiss law, the FDPIC has removed the US from the list of countries that provide an "adequate level of data protection under certain circumstances." This list is merely indicative. In Switzerland there is currently no judicature comparable to the aforementioned CJEU judgment. The Swiss courts' judgment may differ.

Contractual guarantees used in addition to the Privacy Shield regime for data transfer to the US and other third countries lacking an adequacy decision, such as the EU's SCC, which are also frequently used in Switzerland, or "binding corporate rules", cannot prevent foreign authorities from accessing personal data if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency or independent legal protection of the data subjects.

In his aforementioned opinion of 8 September 2020, the FDPIC raised awareness of this problem in the business circles concerned and pointed out a few make-shift solutions such as using one's own encryption or full anonymisation.

The FDPIC advises companies to conduct a case-by-case assessment of the disclosure risks when transferring data to the US based on contractual guarantees. Only that way can they assess the data protection afforded when transferring data to the US and, if necessary, notify

the FDPIC accordingly by furnishing proof. The EU is currently working on a new set of SCC. The FDPIC is monitoring its efforts and will report on the matter in due course.

1.9 International

Introduction

This past financial year, international cooperation was dominated by the COVID-19 pandemic. As it was practically impossible to meet in person, conferences were either cancelled or attended virtually, which presented a number of technical challenges during the set-up period. Without the travel time and cost of meeting in person, the video conferences were attended by more data protection authorities and persons per authority than usual. On the downside, the virtual meetings lacked the opportunities for informal exchanges and networking that are so important for cooperation. The crisis brought home the importance of international exchanges between data protection authorities.

Cross-border data flows continued to expand, largely driven by the pandemic, with ever larger volumes of personal data being transferred abroad directly or stored on clouds or servers abroad. Data subjects are hardly ever aware of which companies or authorities abroad are processing their data. For this reason, it is all the more important to ensure better enforcement of data protection law worldwide, to promote international cooperation among data protection authorities and to work towards a common understanding and harmonised interpretation of international standards and guidelines.

Internationally agreed guidelines make it possible to guarantee the same rights to all data subjects regardless of where they live. Data protection authorities around the world also need to consult among themselves on how to respond to global data protection challenges such as big data, the Internet of Things and artificial intelligence in technical terms and in the performance of their advisory and supervisory roles.

The FDPIC continues his international work and is actively involved in a number of international bodies including, in particular, the Council of Europe, the European and International Conferences of Data Protection Commissioners, the French-speaking Association of Data Protection Authorities and the OECD as well as in cooperation and coordination of the data protection authorities of the Schengen States and in exchanges with the European Data Protection Board (EDPB).

Council of Europe

The Consultative Committee of Convention 108 held six remote sessions on different topics. It adopted Guidelines on Children's Data Protection in an Education Setting and guidelines on facial recognition. The Plenary Meeting also elected the bureau.

On the dates originally scheduled for the Committee's 40th plenary meeting, which had had to be postponed owing to the current health crisis, the Advisory Committee of Convention 108 and the Data Protection Unit organised remote and open sessions to present the work of the Committee to a broader audience than the delegations usually attending the meetings in Strasbourg. Six specific, informative thematic sessions were held on 1, 2 and 3 July:

- Session 1: How to ensure that countries that commit to Convention 108+ comply with its provisions? Why do we need a follow-up and evaluation mechanism, and which one?
- Session 2: How do we address the latest challenges posed by profiling in an AI era?
- Session 3: What does the right to data protection imply in an educational setting? What schools have to do, and what they should stop doing.
- Session 4: Are digital identity programmes being developed in accordance with the "privacy by design" principle?
- Session 5: Mirror of our souls: learning Cicero's lessons and addressing the risks of facial recognition.
- Session 6: Political campaigns and elections: why is data protection crucial?

The Consultative Committee held its 40th plenary meeting – originally scheduled for 1-3 July – by video conference on 18-20 November 2020. During the meeting, the Consultative Committee adopted the revised text of the Guidelines on Children's Data Protection in an Education setting. These guidelines set forth the fundamental principles of children's rights in an education setting and help legislators, policy makers, data controllers and the industry to uphold these rights. The Committee also elected its Bureau members and, among other things, elected Caroline Gloor Scheidegger, head of the Department of International Relations, as FDPIC representative.

Following a written procedure, the Committee of Convention 108 also adopted the guidelines on facial recognition. These offer guidance for legislators and policy makers, emphasising, among other things, the need for the supervisory authorities to be involved. They are also intended as a guide for developers, manufacturers and service providers, pointing out, among other things, that the reliability of the tools used depends on the effectiveness of their algorithm. Furthermore, they provide guidance to entities using facial recognition technology, highlighting their responsibility to conduct an impact analysis on data protection and to implement privacy by design. Finally, the guidelines specify that all data subjects' rights are guaranteed, including the right to information, the right of access, the right to information in the case of automated individual decision-making, the right to object and the right to rectification.

Global Privacy Assembly

The 42nd Global Privacy Assembly (GPA) – formerly known as the International Conference of Data Protection and Privacy Commissioners – took place virtually for the first time on 13-15 October 2020.

The 42nd Global Privacy Assembly Closed Session was opened by Elizabeth Denham, the UK's information commissioner, who highlighted the work carried out by the GPA over the past few years on modernising the assembly, setting the strategic direction and building the capacity of the GPA in order to address the COVID-19-related challenges in 2020.

This year's event was divided into three online sessions, each followed by a discussion. This important annual meeting was attended by more than 100 members.

Day 1 of the conference was devoted, in particular, to reviewing the progress on the GPA strategic plan, agreed on at last year's 41st International Conference in Tirana, namely the key achievements in respect of the three strategic priorities that had been set: advancing global privacy in the digital age, maximising the GPA's voice and influence on the international arena, and capacity building.

Day 2 of the event focused on the challenges posed by the COVID-19 pandemic, stressing the key role and contribution of the GPA COVID-19 Taskforce. The activities of the taskforce were discussed and specific results of its works were presented, notably a compendium of best-practice responses to the COVID-19 pandemic including, for example, the subject of contact tracing.

The first topic discussed on day 3 of the conference was the future of the conference itself. Next, the results of the vote by the GPA members on the working group reports, the report of the executive committee 2020 and the report of the 41st International Conference 2019 were announced: all the reports were adopted.

Five resolutions were adopted on 15 October 2020:

- Resolution on facial recognition technology;
- Resolution on the role of personal data protection in international development aid, international humanitarian aid and crisis management;
- Resolution on accountability in the development and use of artificial intelligence;
- Resolution on the privacy and data protection challenges arising in the context of the COVID-19 pandemic;
- Resolution on joint statements on emerging global issues.

OECD Working Party on Data Governance and Privacy in the Digital Economy

The Working Party continued its work during the year under review, meeting virtually in November 2020. Two topics are worth mentioning: data portability (for which the Secretariat presented the current status for a possible review) and the Secretariat's review of the implementation of the OECD Privacy Guidelines.

Adequate data protection post-Brexit

The UK is still on the list of states whose legislation guarantees adequate data protection as defined in the Swiss Federal Act on Data Protection. Likewise, the UK recognises Switzerland as a country that offers an equivalent level of data protection.

As mentioned in the last Annual Report (see 27th Annual Report, Section 1.9), the UK left the EU (Brexit) on 1 February 2020 after a number of delays. This raised the question of mutual recognition of adequacy. The FDPIC held numerous discussions on the subject with authorities of the Confederation and UK representatives. The discussions continued regularly throughout the current financial year. In parallel, discussions were also held with representatives of the EU Commission following long-running uncertainty over whether or not the EU would still consider the UK to provide adequate data protection from 2021 onwards. For its part, the UK recognised as equivalent, from a legal standpoint, all states that were recognised by the EU as guaranteeing an equivalent level of data protection as at 31 December 2020.

However, as the EU Commission had yet to reach a decision regarding Switzerland's adequacy at the end of 2020, that meant that Switzerland was still recognised by the EU at that point in time. Therefore, under UK law, Switzerland would automatically continue to be recognised, probably for the next four years. That did not mean, however, that Switzerland would automatically grant reciprocal rights.

That said, UK data protection law did not undergo any significant update during the reporting period. Therefore, the country is still on the list of states whose legislation guarantees adequate data protection pursuant to Art. 6 para. 1 FADP. Nevertheless, a review may still be required depending on how UK data protection legislation evolves in the future.

Working group on the role of personal data protection in international development aid, international humanitarian aid and crisis management

At the 42nd Global Privacy Assembly (GPA), the FDPIC presented a resolution on the role of personal data protection in international development aid, international humanitarian aid and crisis management. The resolution was supported by 15 data protection authorities and was adopted unanimously.
The purpose of the resolution is to define the position of GPA members on several of the goals outlined in the Assembly Strategy Plan, specifically those relating to advancing global privacy in the digital age and strengthening relationships with other international bodies and networks advancing data protection and privacy issues.

After the resolution was adopted, it was decided to set up a working group on the role of personal data protection in international development aid, international humanitarian aid and crisis management. The working group has set itself two main objectives:

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

This working group is coordinated by the FDPIC and brings together data protection authorities from around the world as well as the ICRC and the International Organization for Migration.

General Data Protection Regulation

The EU's new General Data Protection Regulation (GDPR) came into force on 25 May 2018. Under certain circumstances, it also applies to data processing by third-country companies. The data protection authorities of Albania, Jersey and Monaco met in Switzerland to discuss numerous questions that remained unanswered.
Adopted on 27 April 2016, the European General Data Protection Regulation (GDPR) has been directly applicable in all EU Member States since 25 May 2018. However, its scope extends beyond the European Union as the provisions of the GDPR are also binding on all non-EU entities (data controllers and processors) providing goods or services to persons resident in the European Union or monitoring the behaviour of those persons, particularly in order to analyse their preferences. The European French-speaking authorities that are not members of the European Union face the same challenges. After a first successful meeting in Monaco in 2018, the FDPIC organised a meeting in Bern in February 2020 for the authorities to discuss the entry into force of the GDPR, to share their experiences and to pool the questions put to them in order to coordinate their responses.

Just over a year after the GDPR came into force, the European Data Protection Board (EDPB) – the inde-

pendent European body which helps ensure the consistent application of data protection rules within the European Union – published its guidelines on the scope of the GDPR. This followed a public consultation held to discuss the guidelines, attended by the FDPIC in collaboration with the Monegasque Data Protection Authority (Commission de contrôle des informations nominatives, CCIN) to seek clarification on a number of aspects of this extremely important issue for third countries that are part of the EU landscape. This new version was also examined and discussed at the meeting. It is clear that numerous questions remain unanswered.

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

The Supervision Coordination Groups held their two meetings via video conference during the year under review. Topics discussed included how to go about the difficult task of finding enough experts from data protection authorities for the Schengen evaluations.

As a national supervisory authority, the FDPIC attended the meetings of the three Supervision Coordination Groups on the EU's SIS II, VIS (chaired by the FDPIC) and Eurodac information systems again this year. The meetings took place via video conference on 17/18 June 2020 and on 25/26 November 2020. The European Data Protection Supervisor (EDPS) and the national data protection authorities of the Member States were represented.

The SIS and VIS Supervision Coordination Groups also addressed the question as to why it was hard to find enough experts from the various data protection authorities for the Schengen data protection evaluation carried out by the European Commission. The EU Commission, which is currently reviewing the Schengen process, organised a video conference on the matter with the data protection authorities of the Schengen States and the European data protection officer in January 2021. A constructive discussion took place on the possible causes and opportunities for improvement. Both sides will examine the possibility of creating a pool of data protection experts for the Schengen evaluations. Furthermore, where possible, the EU Commission will introduce continued education for future data protection evaluation specialists. At its meeting on 18 June, the VIS Supervision Coordination Group re-elected the Commissioner's representative as Chair of the Coordination Group for a further two years.

Freedom of Information

2.1 General

The coronavirus pandemic also affected the implementation of the principle of freedom of information within the Federal Administration. A large number of requests were received from the media and members of the public for specific, transparent information regarding coronavirus-related documents. As well as dealing with a large number of access requests, some authorities faced sometimes complex and extensive enquiries which often required the coordination of different offices and even departments. Overall, implementing the principle of freedom of information during a pandemic proved demanding and challenging at times. Under pressure to act fast, the Federal Administration was subject to high expectations and criticism from the public, while applicants demanded quick and comprehensive access to information in order to understand the government's actions to combat the pandemic, some of which were taken under emergency powers. Nevertheless, the statistics show that, despite the sometimes urgent day-to-day business during the pandemic year, the federal authorities managed to successfully implement the principle of freedom of information within the Federal Administration in the majority of cases.

Furthermore, the figures presented below for the year under review (see Section 2.2) confirm the trends observed in recent years, namely a steady increase in the number of access requests and a consistently high proportion of cases in which full access was granted.

The primacy of oral mediation sessions introduced by the Commissioner in 2017 proved itself again in 2020. At first glance, the figures seem to confirm this only in part: however, this is due to changes to the mediation procedure dictated by the pandemic. At its meeting on 16 March 2020, the Federal Council introduced the obligation to work from home and banned gatherings of more than five people in an attempt to stop the spread of the coronavirus. As a result, the Commissioner was forced to suspend mediation sessions during the first wave of the pandemic (between March and June 2020) and during the second wave for public health reasons and to protect the health of participants.

For the above-mentioned reasons, in many cases, mediation procedures had to be carried out in writing. During the year under review, this working method resulted in a lower proportion of amicable outcomes and longer processing time for mediation procedures, thus creating a backlog. Section 2.3 explains how written mediation procedures have negatively affected processing time and outcome.

Meeting the statutory 30-day deadline for completing a mediation procedure is a challenge at the best of times, let alone in a pandemic. In reality, this deadline is often missed in the case of complex procedures involving three or more parties with requests for access to documents containing information relating to trade secrets or documents about protecting the privacy of private individuals. For a mediation procedure to be carried out, the authorities need to provide the Commissioner with the documents requested by the applicants. The Commissioner is bound by the same obligation of professional secrecy as the authorities whose documents are requested for inspection. In practice, the authorities usually readily hand over the documents to the Commissioner. However, cooperation is not always optimal, as illustrated by one particular case involving the obligation to cooperate in a mediation procedure. According to the principle of freedom of information within the Federal Administration introduced with the Freedom of Information Act, it is no longer up to the Federal Administration to decide at its own discretion whether or not to grant access to information or official documents. The authorities are obliged to cooperate in mediation procedures and are legally required to provide the Commissioner with all the requested documents. In the case in question, the authority refused to hand over the disputed documents to the Commissioner, arguing

that they fell outside the scope of the Freedom of Information Act. The burden of proof being on the authority in question, the latter denied the applicability of the Freedom of Information Act at its own discretion, and so the Commissioner was unable to assess the nature of the documents in question in accordance with Art. 5 FoIA and to determine whether or not there were in fact grounds for dismissal or exceptions as claimed by the authority. As a result, the Commissioner was obliged to recommend granting full access to the requested documents as the authority carrying the burden of proof had to be penalised if it was not prepared to rebut the legal presumption of access to official documents by disclosing them to the mediation authority (see recommendation of 28 January 2021).

As in previous periods, the Administration continued its efforts to introduce new legal provisions establishing further exemptions from the principle of freedom of information. This year we saw this with the COVID-19 Loan Guarantees Act (see Section 2.4).

2.2 Requests for access – further increase in 2020

According to figures provided by the federal authorities, 1193 requests for access were submitted to them between 1 January and 31 December 2020 compared with 916 in 2019 – a 30% increase over the previous year. This figure includes requests for access submitted to the Office of the Attorney General of Switzerland (13) and the Parliamentary Services (6).

This increase is partly due to the large number of requests from people seeking information about the government's actions to combat the coronavirus pandemic. According to the federal authorities, 308 out of 1,193 requests for access (26%) were related to the coronavirus. The authorities compiled statistics on the number of requests for access to coronavirus-related documents. Presented separately in Section 3.3, these statistics show that full access to such documents was granted in 121 cases (39%), namely less often than compared with the overall statistics (see below), while the percentage of requests for access refused outright (38, equal to 12%) was only marginally higher in relation to the overall statistics.

The increase in the number of requests for access submitted is also due to growing public awareness over the years of the principle of freedom of information, due not least to media coverage, with more people taking up the opportunities that it presents. The Commissioner expects this trend to continue in the coming years.

The authorities granted full access to the requested documents in 610 cases (51%), compared with 542 (59%) the previous year, whereas access was partially granted or suspended in 293 cases (25%). In 108 cases (9%), applicants were denied access altogether. According to the authorities, 35 requests for access (3%) were withdrawn, 80 requests were still pending at the end of 2020, and in 67 cases there was no official document. Since 2015, full access to the requested documents has been granted in more than 50% of cases. By comparison, the number of requests for access denied outright remains small, stabilising at around 10% over the years.

Overall, during the pandemic year, the percentage of cases in which full access was granted was 8% lower than in previous years while the percentage of cases in which access was partially granted or suspended was 6% higher. These changes are partly due to the fact that the authorities granted full access to coronavirus-related documents – which, as mentioned, make up roughly a quarter of all requests – in a lower percentage of cases, more frequently granting partial access, suspending access or denying access altogether.

Federal departments and federal offices

Various administrative units were the focus of much media and public attention in 2020 in connection with the coronavirus pandemic. Due to the nature of their work, the FOPH, the DDPS and the FDF, in particular, received a large number of requests for access to information. The authorities in question reported that the requests were sometimes complex and extensive: in many cases they required time-consuming coordination between federal offices and departments, for example in the case of documents relating to the procurement

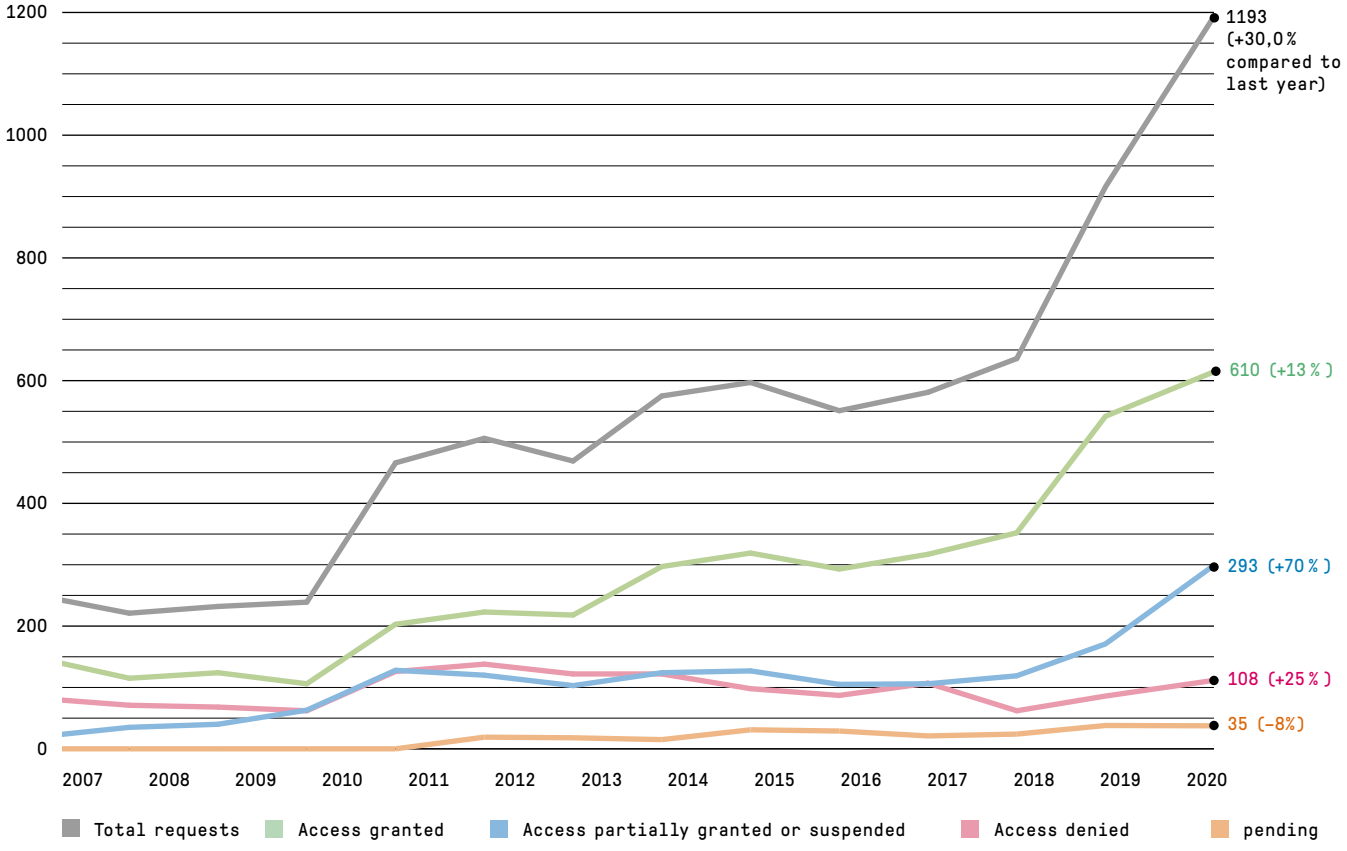
of medical supplies. Understandably, these authorities had a heavier workload than in previous years.

The figures released by the federal offices indicate that the FOPH received the most requests for access in 2020, namely 181 – 134 of which for access to coronavirus-related documents (see Section 3.3) – followed by the FOSPO with 150, swissmedic with 42 and the FOEN with 38 requests. The departments which received the most requests are the FDHA (312) and the DDPS (251). Conversely, 13 authorities informed us that no requests for access had been submitted to them during the year under review. The Commissioner himself received ten requests. He granted full access in eight cases; in one case, the requested document did not exist, and one case was still pending at the end of 2020.

In 2020, fees charged for obtaining access to official documents totalled CHF 15,189, a lower total than the previous year (CHF 18,185). Only in two cases was a total fee of CHF 450 charged for access to coronavirus-related documents.

While the FDJP and the Federal Chancellery did not charge any fees, the other six departments did invoice applicants for some of the time spent dealing with their requests (FDHA: CHF 4,643; EAER: CHF 3,786; DETEC: CHF 3,310; FDF: CHF 1,900; FDFA: CHF 900; DDPS: CHF 650). It is important to note that just 25 out of 1193 requests for access incurred a fee. Compared with the previous year, when fees were charged in 31 cases, both the number of cases in which a fee was charged and the total amount charged were lower. This is remarkable considering that the number of requests for access was (again) much higher. As in previous years, fee-charging is the exception, with access being

Figure 1: Evaluation of requests for access – trend since 2006



granted free of charge in almost 98% of cases. The day-to-day administrative practices support the principle of free access to official documents as proposed by the National Council Political Institutions Committee (see Section 2.4, Opinion of the FDPIC).

As regards working hours spent processing access requests, the Commissioner reiterates that the authorities are under no obligation to record these hours and that there are no directives establishing a standard recording procedure applicable to the entire Federal Administration. Data is sent to the Commissioner on a purely voluntary basis and only partially reflects the working hours actually spent handling requests. According to the data received, the working hours published this year were 5,010 hours, up from 2019 (4,375 hours). Therefore, the increase in the number of access requests (30%) does not match the increase in the amount of time spent handling the requests (15%). The working hours devoted to preparing for mediation sessions also increased, totalling 569 hours (compared with 473 hours in 2019).

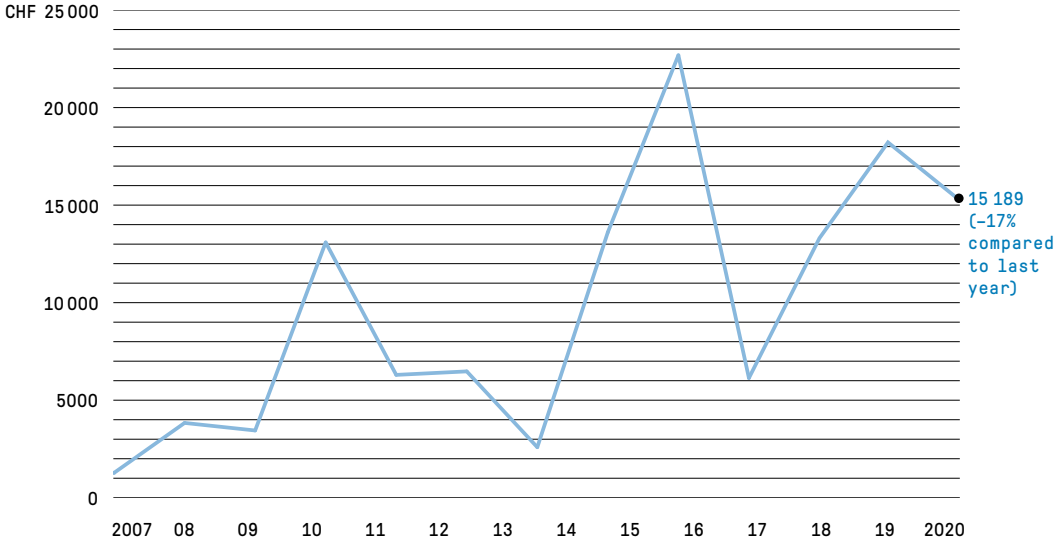
Parliamentary Services

The Parliamentary Services informed us that they had received six requests for access: in one case, the requested document did not exist, while the other five requests were denied outright.

Office of the Attorney General of Switzerland

The Office of the Attorney General of Switzerland announced that it had received 13 requests in 2020. Full access was granted in six cases, and access was denied outright in one case. As for the remaining cases, there was no official document in two of them, and four cases were still pending at the end of the reporting year.

Figure 2: Fees charged since the FoIA entered into force



2.3 Mediation procedure – fewer mediation requests

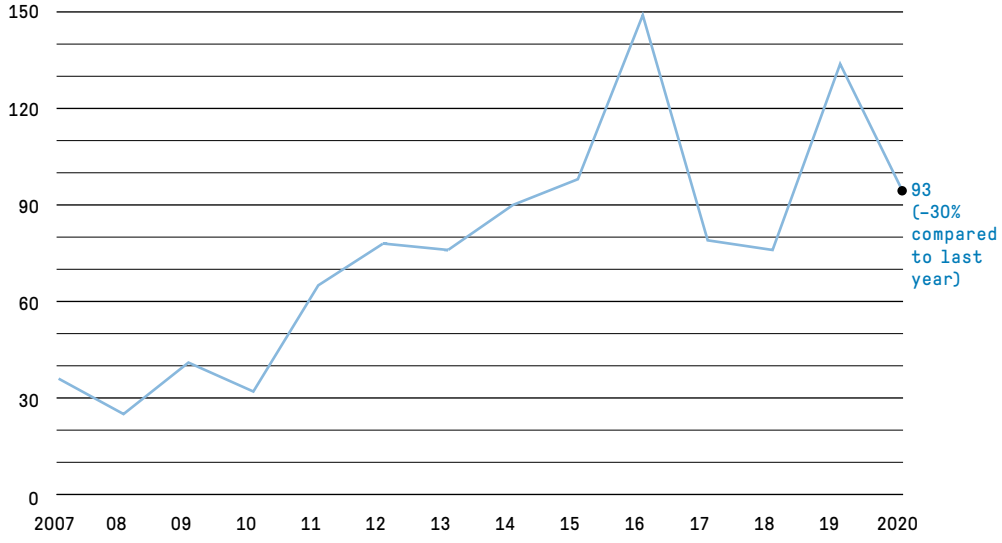
In 2020, the Commissioner received 93 mediation requests, 30% fewer than in 2019 (133, whereby 28 procedures concerned the same matter). The majority of mediation requests was submitted by private individuals (42) and the media (31). From these figures, we can deduce that, of the 401 cases in which the Federal Administration fully or partially denied access, 93 (23% of all unmet requests for access) resulted in a mediation request being submitted to the Commissioner. Twenty-four of these (26%) concerned coronavirus-related documents.

In 2020, 119 mediation requests were settled, of which 79 had been submitted during that year and 40 the previous year. In 40 cases, the participants were able to reach a consensual solution. The Commissioner also issued 27 recommendations, enabling him to close 55 cases which were unlikely to result in agreement between the parties.

The cases dealt with included 11 mediation requests which were not submitted on time, 12 cases which did not satisfy the conditions for the application of the Freedom of Information Act, and one request that was withdrawn.

At the end of the year, eight mediation procedures had been suspended by agreement between the participants.

Figure 3: Mediation requests since the FoIA entered into force



Proportion of amicable outcomes

There are numerous advantages to amicable solutions: for instance, they accelerate the procedure for access to documents and lay the foundations 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 mediation sessions.

During the year under review, 40 amicable outcomes were achieved, and 27 recommendations were issued by the Commissioner to settle 55 cases. Therefore, the ratio of amicable outcomes to recommendations is 34%, which is significantly lower than previous years.

As mentioned in Section 2.1, mediation sessions could not be held between March and June 2020 because of the coronavirus pandemic, and so 13 sessions had to be cancelled. Amicable solutions are typically only reached in mediation sessions. Therefore, during the year under review, in the 40 mediation sessions that did take place, an agreement was reached in 24 cases (60%), in line with data for previous years.

This year, the Commissioner issued recommendations in what seems like a large number of mediation procedures compared with previous years but this is mainly due to a statistical anomaly: Two requests for access resulted in mediation requests being submitted by an unusually large number of third parties (ten third parties in one case and 18 in the other). More than half of these 28 mediation requests resulted in a recommendation being issued.

In conclusion, the Commissioner commented on how effective oral mediation procedures were in swiftly reaching amicable solutions. In some cases, because of the coronavirus measures in place, participants requested that the procedure be suspended until oral mediation sessions could be resumed.

All the recommendations issued are available on the Commissioner's website.

Table 1: Amicable outcomes

2020	**34 %**
2019	61 %
2018	55 %

Duration of mediation procedures

Table 2 is divided into four sections according to the time it took to settle the procedures. It should be noted that the processing time 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 proceedings are extended.

Table 2 shows that 43% of mediation procedures completed in 2020 were concluded within the 30-day period, while 30% took between 31 and 99 days to process, and 27% took 100 days or more.

Failure to meet the deadline is often due to unavailability of the people or authorities concerned (due to holidays, illness or travel), the large number of third parties involved in the procedure, or the need to resolve complex legal issues. In the year under review, delays were compounded by the restrictions imposed on the parties and staff by the pandemic. These explanations also apply to the 32 cases that took 100 days or more to process, including one case in which ten procedures were consolidated and another in which 18 were consolidated. Consultations conducted abroad, multiple negotiation rounds among the participants, and the involvement of a large number of documents or people were other factors that made it hard to meet deadlines. The above-mentioned situations frequently entail a substantially higher workload, and in such cases – in accordance with Article 12a of the Freedom of Information Ordinance (FoIO; RS 152.31) – the Commissioner may extend the deadline by a reasonable period. During the year under review, under severe pressure due to

Table 2: Processing time of mediation procedures

Processing time in days	Period 2014–August 2016*	Pilot phase 2017	Pilot phase 2018	Pilot phase 2019	Pilot phase 2020
within 30 days	11 %	59 %	50 %	57 %	43 %
from 31 to 99 days	45 %	37 %	50 %	38 %	30 %
more than 100 days	44 %	4 %	0 %	5 %	27 %

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

the coronavirus pandemic, the authorities were granted deadline extensions in numerous mediation procedures.

In most cases, the statutory 30-day deadline for completing the mediation procedure can be met, provided the mediation sessions are held according to schedule – i.e. without the parties requesting any postponements – and culminate in agreement within the time limit from receipt of the request. If no agreement is reached, the Commissioner cannot always issue his written recommendation to the parties within 30 days of receipt of the request.

The higher proportion of written mediation procedures and written recommendations due to the pandemic significantly increased the Commissioner's workload, resulting in longer processing time for the procedures and a processing backlog. With another lockdown at the beginning of 2021, the Commissioner can expect the backlog to increase further.

Furthermore, third parties interviewed involved legal representatives again this year at the access and mediation procedure stages, which is not conducive to a straightforward, pragmatic and swift solution.

Number of pending cases

The figures below indicate the number of pending cases at the end of the year under review. As at January 2021, the number of mediation cases still pending from 2020 stood at 17, including eight suspended procedures (three from 2019 and five from 2020). Seven cases had been completed by the time of going to press.

Table 3: Pending mediation procedures

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

CORONA

Legislative process for the transposition of the COVID-19 Loan Guarantees Ordinance into the COVID-19 Loan Guarantees Act

Under the COVID-19 Loan Guarantees Act, the identities and bank details of companies and individuals seeking loans and the size of the loans granted or refused within the context of the federal loan guarantee programme are to be kept secret. The Commissioner had unsuccessfully opposed this restriction of the principle of freedom of information during the legislative process.

On March 2020, the Federal Council introduced a temporary emergency ordinance facilitating access to bridging loans for many eligible companies to provide the liquidity needed to help them through the crisis caused by the pandemic. The content of the emergency ordinance was transposed into an urgent temporary federal act, which was adopted by Parliament in December 2020.

Under Art. 12 para. 2 of the COVID-19 Loan Guarantees Act (Covid-19-SBüG), personal data and information regarding companies and individuals that have applied for and been granted loans may not be disclosed insofar as they contain their identity and bank details or the size of the loans granted or refused. According to the dispatch on the Covid-19-SBüG, this is a special provision within the meaning of Art. 4 FoIA, which means that this information falls outside the scope of the Freedom of Information Act and is therefore not accessible on request. The Commissioner had objected to the introduction of this special provision in both the consultation on the Covid-19-SBüG and the subsequent office consultation on the dispatch and draft legislation. He also pointed out the goals pursued with the Freedom of Information Act such as ensuring transparency of governance and preventing mismanagement and corruption. In his view, the unconditional secrecy of the information in question was inappropriate given that 40 billion francs of taxpayers' money were being spent. Any losses on the loans granted would need to be covered by taxpayers' money. Following the objections raised in connection with the Administration's handling of the provision of guarantees in deep-sea shipping, the Commissioner is surprised that Parliament has enshrined the secrecy proposed by the Federal Council in the act passed on 19 December 2020.

In the consultation procedure, the Commissioner had pointed out, in vain, that justified private interests remained protected even where the Freedom of Information Act applied. The act explicitly guarantees the protection of business secrets (Art. 7 para. 1 let. g FoIA) and of the privacy and personal data of natural persons and legal entities (Art. 7 para. 2 FoIA, Art. 9 para. 2 FoIA and Art. 19 FADP). The Commissioner also stated that banking secrecy took precedence over the Freedom of Information Act according to established doctrine and case law. Equally unsuccessfully, the Commissioner referred in his opinion to the Federal Act on Financial Assistance and Subsidies (Subsidies Act) and the Federal Act on Financial Aid to Guarantee Organisations for SMEs. Although the two acts present clear similarities with this legislation, they do not contain any special provisions within the meaning of Art. 4 FoIA.

Office consultation on the Federal Council's draft opinion on the National Council Political Institutions Committee report of 15 October 2020 on the Graf-Litscher parliamentary initiative 16.432. Charging system. Principle of freedom of information in the Federal Administration

The National Council Political Institutions Committee has drafted a proposal according to which access to official documents should, in principle, be free of charge, with fees charged only in exceptional circumstances. The Federal Council wants to be allowed to set the maximum fee amount itself in the ordinance, whereas the Commissioner is in favour of enshrining the maximum amount directly in the Freedom of Information Act.

The parliamentary initiative 16.432 ("Charging system. Principle of freedom of information in the Federal Administration") seeks to modify the legal basis in the Freedom of Information Act so as to provide access to official documents free of charge.

The National Council Political Institutions Committee (PIK-N), in charge of the matter, approved a preliminary draft amendment to the Freedom of Information Act, which it revised after consultation and submitted to the National Council. According to the draft, the principle of free access to official documents is to be enshrined in the Freedom of Information Act. Only in exceptional cases may a fee be charged, namely "when a request for access requires a particularly time-consuming assessment by the authority". The Committee majority feels that a maximum fee of CHF 2,000 should be set out in the Freedom of Information Act, while the Federal Council should define the details and set the rates depending on the time required. A minority feels that the Federal Council should also be allowed to set a maximum fee.

The Commissioner supported the Committee majority's proposal to set out a maximum fee directly in the Freedom of Information Act because, on a legal level, this would ensure that the fees occasionally charged never reached proportions that would hinder access to official documents. Now that the Federal Council has decided not to enshrine the determination of the fee level in the act, it is up to the National Council to decide on the matter.

Revision of the Federal Act on the Promotion of Research and Innovation (RIPA). Office consultations in preparation for the Federal Council dispatch

In the consultation procedure on the revision of the RIPA, a request was made to tighten the rules on disclosure of the names of the referees and scientific reviewers in the appeal procedure. However, the Commissioner opposed the request.

In appeals concerning denied research contributions, Art. 13 para. 4 RIPA states that the names of the referees and scientific reviewers may only be communicated with their consent to the complainant on request. In its ruling A-6160/2018 of 4 November 2019 in reference to an appeal under the Freedom of Information Act, the Federal Administrative Court construed Art. 13 para. 4 RIPA to mean that said names may only be communicated to third parties if the referees and reviewers in question have expressly given their consent. According to the Federal Administrative Court, this is a special provision within the meaning of Art. 4 FoIA, which means that the Freedom of Information Act does not apply.

However, according to the court, Art. 13 para. 4 RIPA does not constitute a general duty of confidentiality.

In the consultation procedure on the revision of the RIPA, the Swiss National Science Foundation (SNSF) requested that the rules on disclosure be tightened so that only the complainant may request the names in question. The Commissioner then successfully argued against including the issue in the bill with the Swiss State Secretariat for Education, Research and Innovation (SERI) in charge of the matter.

In the Federal Council's dispatch of 17 February 2021, the proposed tightening of the rules on disclosure was dropped.

Partial revision of the HIA regarding cost-containment measures (Package 2)

The Federal Office of Public Health (FOPH) is preparing a partial revision of the HIA regarding cost-containment measures. Among other things, the draft act introduces an exception to freedom of information in respect of all documents relating to pharmaceutical pricing models in the health insurance industry. The Commissioner opposes the plan.

In the 27th Annual Report 2019/20 the Commissioner reported that a consultation procedure would be initiated for a partial revision of the Health Insurance Act: the consultation took place during the year under review. The Commissioner had opposed the FOPH's plan to deny the public the right to inspect documents relating to pharmaceutical pricing. In the Commissioner's view, the prices of medicines covered by compulsory health insurance and the documents used to set the prices should remain accessible to the public. If not, this would lead to untransparent practices in relation to the inclusion and review criteria in respect of the list of pharmaceutical specialties and the refund mechanism. Members of the public and rival companies should be allowed to continue to monitor and understand the FOPH's approval process. The outcome of the consultation procedure is not yet known at the time of going to press.

During the year under review, the Commissioner carried out a mediation procedure regarding FOPH documents relating to pharmaceutical pricing in compulsory health insurance. Specifically, access was requested to information on pharmaceutical pricing models. As the FOPH and the applicant failed to reach an agreement during the mediation procedure, the Commissioner had to issue a written recommendation. The FOPH's main justification for refusing to disclose the requested documents was that, without secrecy, security of supply could no longer be guaranteed for innovative, high-priced medicines. In his recommendation, the Commissioner stated, among other things, that, in his view, the current Freedom of Information Act left no room to anticipate the Federal Council's planned changes to the law. As the FOPH did not provide for any exceptions to be made under the current Freedom of Information Act and was therefore unable to rebut the legal presumption of access to the requested information, the Commissioner recommended that full access be granted.

New Federal Act on General Aspects of the Collection of Charges and on Checks on the Cross-Border Movement of Persons and Goods by the Federal Office for Customs and Border Security (FOCBS Enforcement Task Act)

In the last quarter of 2020, the Federal Customs Administration (FCA) carried out a consultation procedure on the introduction of a new FOCBS Enforcement Task Act. All restrictions on the principle of freedom of information have been removed from the draft legislation.

In the 27th Annual Report 2019/20 the Commissioner reported on the office consultation on the opening of a consultation procedure for a new Federal Act on Customs and Border Security. The draft legislation was revised after the office consultation and is now referred to as the "Bundesgesetz über den Allgemeinen Teil der Abgabenerhebung und die Kontrolle des grenzüberschreitenden Waren- und Personenverkehrs durch das Bundesamt für Zoll und Grenzsicherheit (BAZG-Vollzugsaufgabengesetz)" (Federal Act on General Aspects of the Collection of Charges and on Checks on the Cross-Border Movement of Persons and Goods by the Federal Office for Customs and Border Security (FOCBS Enforcement Task Act)). The FCA took on board the Commissioner's concerns and deleted the originally envisaged restrictions on the principle of freedom of information. The consultation procedure was only carried out in the year under review.

The FDPIC

3.1 Duties and resources

CORONA

The pandemic

The data processing projects aimed at fighting the current pandemic – conducted within a short time frame due to the health crisis – and the increased demand for public documents have placed extraordinary pressure on all staff.

The FDPIC is a federal enterprise affiliated to the Federal Chancellery for administrative purposes, and as such it has implemented all the Federal Council's guidelines aimed at protecting employees during the pandemic. Accordingly, the FDPIC's staff worked predominantly from home during the year under review. Face-to-face meetings were possible only for a few weeks, making the recruitment and supervision of new staff particularly difficult.

Services and resources in the field of data protection

Number of staff

Between 2005 and 2019, the total number of staff responsible for implementing the Federal Act on Data Protection (FADP) fluctuated between 20 and 24 FTEs. One reason for the variation is the Freedom of Information Act (FoIA), which came into force in 2006. Since the Federal Council did not approve additional staff positions as planned, the FDPIC was required to use his existing staff and, in some cases, the Federal Chancellery's resources. Though additional staff positions were approved when Switzerland joined Schengen and Dublin and when special laws in the health sector were passed, they could not all be filled because of general spending cuts.

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 (BBI 2017 7172). Switzerland's new Federal Act on Data Protection related to 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 the new duties and powers. This increased the headcount to 27 FTEs in 2020. In spring 2021, the FDPIC asked the Federal Council to create six new FTEs in view of the forthcoming entry into force of the revised FADP in 2022.

Due to retirements and other departures, the department's age structure has become younger in recent years, easing the pressure on the staff budget.

Table 4: Number of staff to be used for FADP concerns

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27

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 (NMM): consultancy, supervision, information and legislation. During the reporting year running from 1 April 2020 to 31 March 2021, the staff resources available at the FDPIC for data protection were allocated to these groups as follows:

Table 5: Services in data protection

Consultancy – private persons	24,8 %	
Consultancy – Federal Administration	20,1 %	
Collaborations with Cantons	1,8 %	
International Cooperation	11,1 %	
Total Consultancy		**57,8 %**
Supervision	15,0 %	
Certification	0,1 %	
Data collection register	0,4 %	
Total Supervision		**15,0 %**
Information	17,0 %	
Education, speeches and presentations	2,4 %	
Total Information		**19,4 %**
Legislation	7,3 %	
Total Legislation		**7,3 %**
Total data protection		**100,0 %**

Consultancy

As set out in the opening section on "Current challenges and priorities", the FDPIC continues to face a consistently high demand for consultancy services as he is required to oversee large digital projects. The proportion of staff working in consultancy has increased by around 7% to 57.8%. In the FDPIC's inspection plan for 2021, 15 large projects are currently receiving support in the form of consultancy. Six of these projects are related to the digital transformation of the Federal Administration ordered by the Federal Council, whereby efforts are being made to reduce the digitalisation backlog that politicians and the media have drawn attention to as a result of the ongoing pandemic.

The FDPIC's resources remain tight given the legal and technological risks that the dynamic progress of digitalisation poses. Therefore, he was unable to provide timely support to the extent required to fully meet the increased demand for project consultancy again this year. During the reporting period, three teams from the Data Protection Directorate responded to around 60 enquiries and complaints from members of the public each month with a standard letter referring the people concerned to the option of civil proceedings. This is causing mounting confusion, because the EU's General Data Protection Regulation requires EU data protection authorities to investigate all complaints from members of the public. Moreover, the fully revised FADP also stipulates a wider-ranging obligation for the FDPIC to directly handle individual complaints from Swiss persons.

Big data and artificial intelligence are becoming a business model in all sectors, and the FDPIC is required to provide supervision in an increasingly large number of domains due to growing technical risks to privacy. This means the number of large data processing projects run by businesses and state authorities is set to continue to grow, following the trend of previous years.

Table 6: Consultancy for large-scale projects in 2021

Fundamental rights	5
Finance	1
Health / Employment	3
Telecommunications	1
Commerce and economy	2
Federal archives	1
Migration	1
Customs	1
Total	**15**

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. Our current staffing levels severely limit the frequency of inspections. In 2018, around 12% of staff resources were used for supervisory duties, which was significantly below the long-term average of around 20%. In the last reporting periods, this proportion was at least prevented from falling below 15%. Our inspection plan for 2021 shows that 13 comprehensive inspections can be carried out with these resources. Compared with the volume of work carried out by the federal bodies and the number of large and medium-sized companies (around 12,000) and foundations and associations (around 100,000) in Switzerland, the current frequency of inspections remains low. Explaining to the media and consumer protection organisations that the FDPIC's limited resources make him reluctant to open formal investigations remains a difficult task for the Commissioner. Public expectations in the run-up to the entry into force of the revised FADP are high, placing increasing pressure on the FDPIC. Therefore, the FDPIC hopes that the Federal Council will create the six requested staff positions.

Legislation

The changes in the way personal data is processed which are to be introduced in connection with the digital transformation of the federal offices are only permissible if specifically authorised in legislation. This entails a large number of new and revised provisions on data processing in federal law, on which the FDPIC has expressed his views in various consultation procedures. Despite the amount of extra work and the time-consuming revision of the FADP and the corresponding ordinance, in the last reporting periods we managed to keep our supervisory workload low, for example by limiting the number of detailed opinions on key projects.

Complete revision of the FADP

In the run-up to the implementation 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. The creation of three staff positions by the Federal Council with the implementation of the new FADP has allowed the FDPIC to forge ahead with his work.

Participation in committee consultations and parliamentary committee hearings

During the year under review, the PIC-N invited us twice in April 2020 to discuss a coronavirus-related application of Swisscom for visualising gatherings. In addition, the committee sought our input at the beginning of May on the launch of the coronavirus warning app. Around the same time, the PIC-S consulted us on both the revision of the FADP (resolution of differences) and the partial revision of the OASI (AHV) Act in connection with the use of the OASI number. At the end of May, the PIC-S consulted the FDPIC twice on the urgent amendment of the Epidemics Act. Before inviting us for the resolution of differences in connection with the revision of the FADP in July 2020, the same committee consulted us on this revision and on the revision of the OASI Act. In July this year, we were invited by the FDJP/FCh sub-committees of the CC to present our annual report.

Other interviews were held this year to discuss the electronic patient record with the CC-N and in connection with the PIC-S survey on data protection in healthcare during the youth session.

Finally, the PICs of both chambers invited us to attend five meetings, and the SSHCs of both chambers invited us to attend two meetings, which focused on facilitations for vaccinated people and other COVID-19 issues.

Assessment criteria

Whether and to what extent the FDPIC is allocated additional resources is a matter for the political authorities to decide. Their discretionary judgements play a significant role in assessing current and future digitalisation trends and the impact of these trends on the FDPIC's activities. The FDPIC's central role is to protect people's privacy and to ensure that they retain ultimate control of their information in our digital society. The FDPIC must be able to act autonomously.

This requires appropriate and sufficient resources in terms of staff, materials, technology and funds. Its supervisory division should not be limited to reacting to essential matters: instead it should be able to take the initiative with the credibility and thoroughness which affected members of the public can reasonably expect in defence of their basic rights.

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

Services and resources in the field of freedom of information

Having undertaken a year-long trial in 2017, the Freedom of Information unit – which had 4.4 staff positions during the year under review – has begun to follow a faster, shorter procedure in which disputes are normally settled orally. This procedure continues to work well, in that the proportion of disputes settled amicably has remained high over the years, and, in most cases, statutory time limits were only exceeded in cases where the procedures and content were complicated.

Due to the pandemic and the measures taken by the Federal Council to protect public health, disputes could not be settled orally for several months in both the year under review and the current year. During that time, the Commissioner had to revert to the written procedure. This impacted negatively on the time needed to process individual procedures, which, combined with the still very large number of mediation requests – some of which were complex and extensive – resulted in a processing backlog. The current reporting year has shown once again that when numerous requests are submitted within a short time span and vacant positions go unfilled, the unit quickly falls behind, making it harder to meet the statutory time limits for completing the dispute resolution procedure (see Section 2.2).

The trend in the increase of mediation requests looks set to continue in 2021, and the backlog is likely to make it increasingly difficult to process new cases within the statutory time limits with the resources available.

Table 7: Outcome objectives FDPIC

Outcome groups	Outcome objectives
Consultancy	The consultancy 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.
Legislation	The FDPIC has an early say on and acitvely influences all special norms and regulations created at national and internationala level. He helps the parties affected to formulate rules of good practice.


OPEN
RIDE

3.2 Communication

Communications dominated by the pandemic

The beginning of the year under review practically coincided with the outbreak of the coronavirus pandemic in Switzerland. The topic remained the focus of attention throughout the year and beyond. The Commissioner's communication work centred on identifying relevant data privacy risks and raising public awareness. Although the Commissioner generally acts independently, on many occasions it was deemed necessary and useful for him to consult the authorities in order to provide coherent information to the public during the crisis. On occasion, his communication work also involved exchanges with the cantonal data protection officers.

Regardless of the pandemic, the increased pace of digitalisation and globalisation of society has compounded privacy concerns. As a result, the FDPIC had to continue his work of raising media and general public awareness on the pressing issues of privacy protection and the principle of freedom of information within the Federal Administration.

Finally, the focus was on the parliamentary debate on the new Federal Act on Data Protection, which the Commissioner closely monitored and which concluded in September 2020 with the law being passed by both chambers. No referendum was called against the fully revised FADP. We published a short commentary on the new provisions on our website (see Focus 1). When the Act comes into force, the FDPIC will have new tasks and strengthened supervisory powers, which is expected to increase the need for communication further and require a greater public presence. The existing fact sheets, explanations and guidelines are being revised in view of the implementation of the new Act and corresponding ordinance.

Communication challenges and conditions

In the second half of 2020, the Communications department returned to its original number of staff, namely 2.4 full-time equivalents, shared between three persons, whereby Switzerland's multilingualism is now better reflected again in the posts filled. Due to limited resources, the Commissioner's public relations work focuses on three key communication channels: the Annual Report (this document), the website and direct relations with the media. Twitter is used to a limited degree, while other social media platforms are avoided, not least for data protection reasons.

During the year under review, we put our Annual Report out to tender. This allowed us to improve the editorial and conceptual framework while keeping costs the same.

Media interest remains high

Strong media interest during the year under review was reflected in the large number of opinions issued by the Commissioner and the Communications department on current enquiries and in the numerous articles and posts (printed and digital) on the general topic of data protection and the principle of freedom of information within the Federal Administration. In our media monitoring alone (covering the Swiss media and a selection of key international printed publications), we recorded approximately 4,000 posts, around twice as many as the previous year – an increase that cannot be explained by changes to the search profile but rather points to significantly higher relevance. More than half of all posts related to the coronavirus pandemic.

At the same time, we witnessed a great deal of activity on social networking sites (social media and online platforms; see Key figures on back cover). The FDPIC was mentioned 7320 times: in 1152 instances, the Commissioner or a spokesperson was quoted directly. More than half of all mentions were on channels abroad. Engagement is a key performance indicator in social media and measures the number of activities such as likes, shares and comments per post. Engagement was very high at 3.36, pointing to increased active networking within communities.

We handled around 600 media enquiries in total – around one third more than the previous year. Most of the people who contacted us were accredited journalists at the Federal Palace Media Centre. Members of the public and companies used email, post

or our telephone hotline to address their concerns and questions to our experts, and we received a total of around 4,200 enquiries via these channels.

The Commissioner attended around forty events again this year. The organisers of these events included associations and clubs, educational establishments, public authorities, and companies, as well as organisations involved in digitalisation.

Opinions, recommendations and publications

During the year under review, the Commissioner published a range of opinions and statements on current projects and events relating to the coronavirus (see box) as well as the following subjects in particular:

- Consultancy and the provisions of the fully revised Federal Act on Data Protection;
- Insufficient regulation of data processing in the new customs police act;
- Swiss-US and EU-US Privacy Shields, in particular the ruling by the Court of Justice of the EU (CJEU) on European standard contractual clauses;
- Data processing by Diem (formerly Libra);

Revision of the HIA: FDPIC advocates transparency of pricing models.

On the FDPIC's website we also published 26 recommendations regarding the principle of freedom of information.

The 27th Annual Report 2019/2020 was published on 30 June 2020 in accordance with the provisions of Art. 30 FADP. It was published in four languages again this year and is available both in printed form and as an ePaper linked on the website.

CORONA

Coronavirus update

As well as offering extensive consultancy services during the pandemic, on several occasions the Commissioner and his experts made public their position regarding data protection compliance in connection with key challenges, for example in relation to the following subjects:

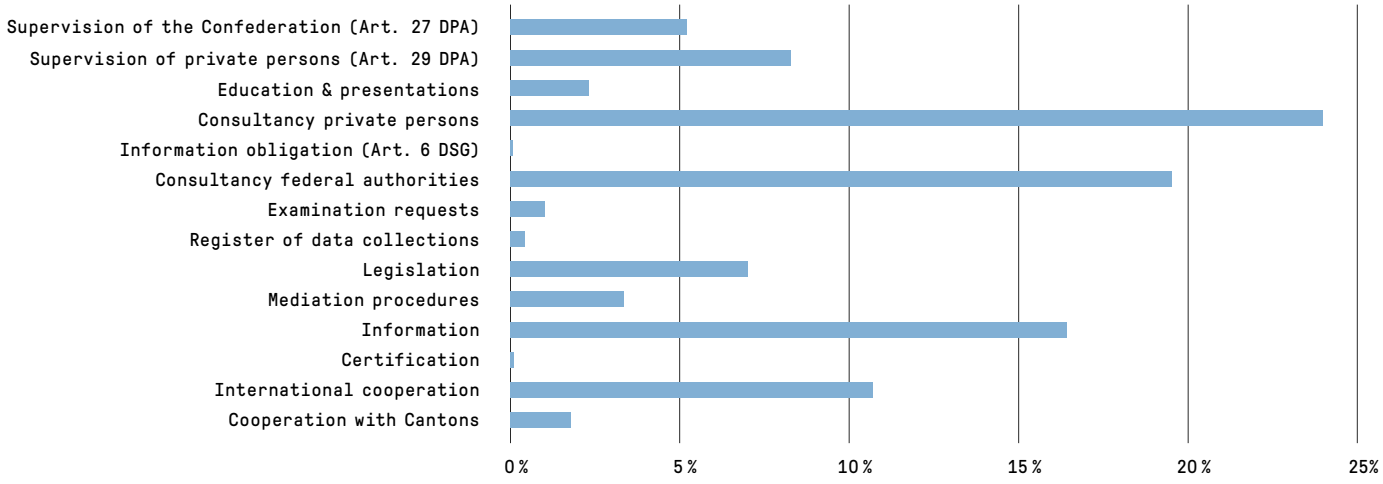
- Analysis of mobility behaviour across Switzerland: the FOPH's access to Swisscom location data
- Proximity tracing app: privacy compliance of SwissCovid app
- Measures for the safe use of audio and video conferencing systems
- Coronavirus protection schemes of private operators: voluntary disclosure of personal details
- Guest lists and contact details: operators must guarantee data protection when collecting contact details; voluntary use of apps
- Procedure against myvaccines foundation and vaccination platform

On International Data Privacy Day (28 January 2021), the FDPIC and Privatim – the Association of Swiss Commissioners for Data Protection – reiterated the need to protect privacy during the pandemic. Addressing the media, the data protection authorities affirmed individuals' right to privacy and self-determination, which must not be restricted after the current pandemic subsides. The public must continue to have a genuine right of choice regarding digital technologies, enabling them to opt for anonymous alternatives.

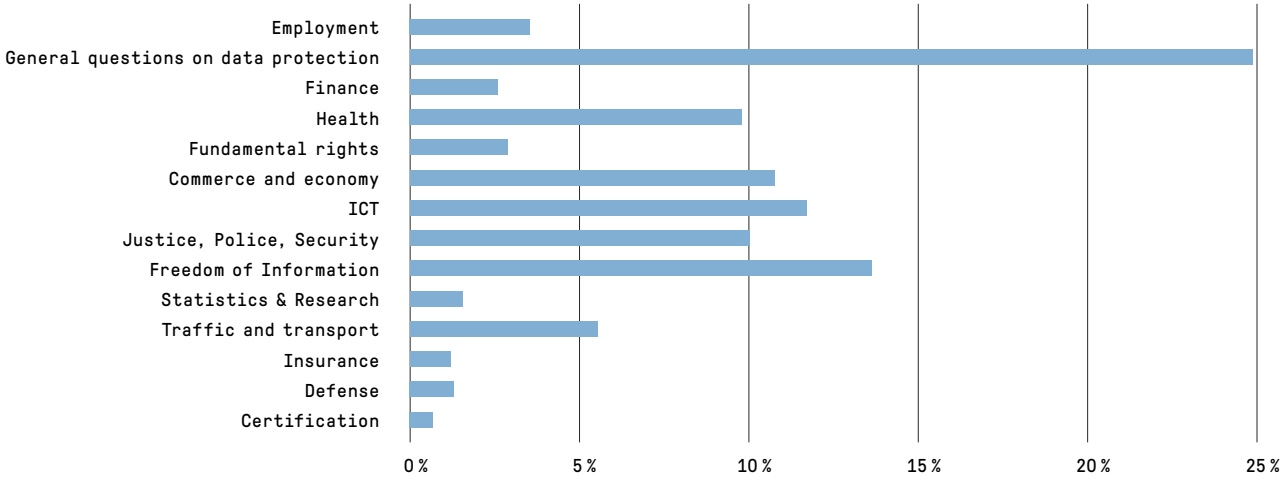
3.3 Statistics

Statistics on FDPIC's activities from 1st April 2020 to 31 March 2021 (Data protection)

Workload per tasks

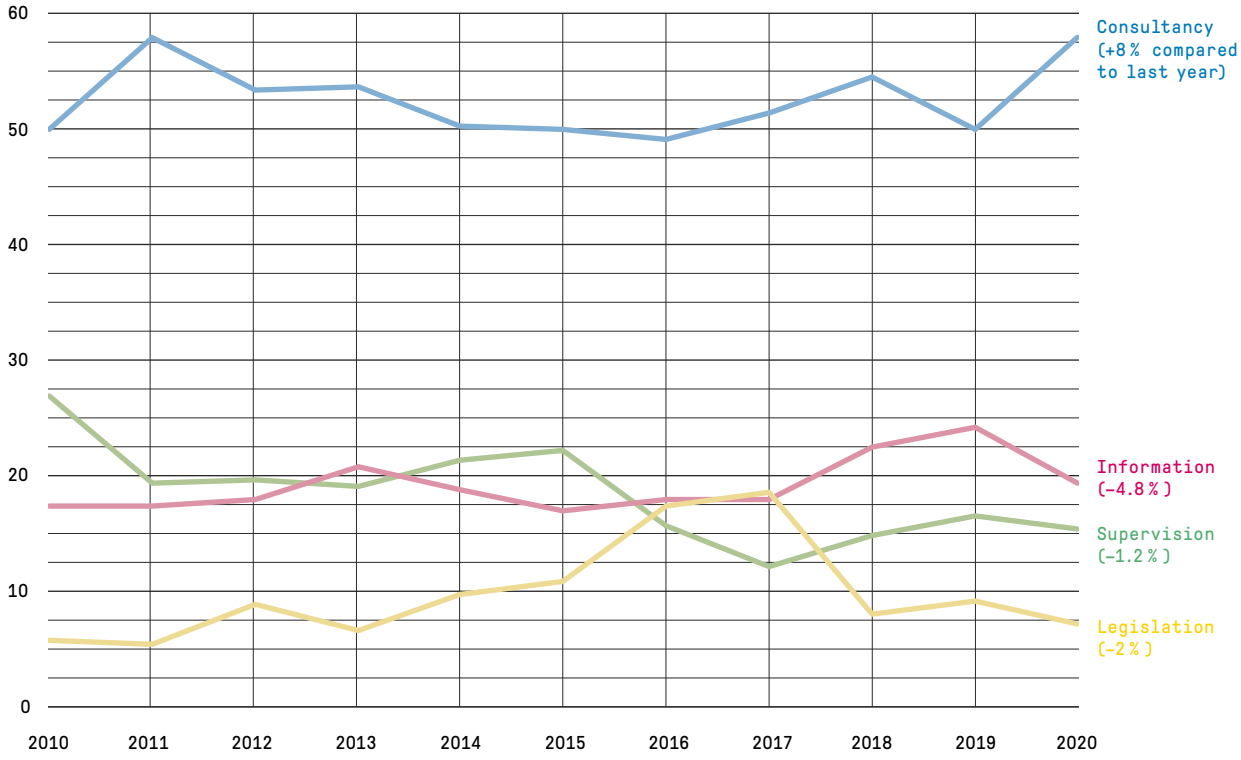


Workload per material



Multi-year comparison

(as a percentage)



Overview of applications from 1st January to 31 December 2020

Department	Number of requests	Access completely granted	Access completely denied	Access partially granted//suspended	Request withdrawn	Pending requests	No document available
FCh	31	20	5	4	0	2	0
FDFA	174	88	14	47	11	4	10
FDHA	312	114	26	100	8	41	23
FDJP	77	45	11	9	2	3	7
DDPS	251	184	10	37	5	10	5
FDF	109	51	13	28	3	6	8
EAER	115	49	15	36	3	7	5
DETEC	105	53	8	32	3	3	6
OAG	13	6	1	0	0	4	2
PS	6	0	5	0	0	0	1
Total 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Total 2019 (%)	916 (100)	542 (62)	86 (11)	171 (21)	38 (6)	43 (5)	36 (4)
Total 2018 (%)	636 (100)	352 (55)	62 (10)	119 (19)	24 (4)	48 (7)	31 (5)
Total 2017 (%)	581 (99)	317 (55)	107 (18)	106 (18)	26 (4)	21 (4)	–
Total 2016 (%)	551 (99)	293 (53)	87 (16)	105 (19)	33 (6)	29 (5)	–
Total 2015 (%)	597 (100)	319 (53)	98 (16)	127 (21)	31 (5)	22 (4)	–
Total 2014 (%)	575 (100)	297 (52)	122 (21)	124 (22)	15 (3)	17 (3)	–
Total 2013 (%)	469 (100)	218 (46)	122 (26)	103 (22)	18 (4)	8 (2)	–
Total 2012 (%)	506 (100)	223 (44)	138 (27)	120 (24)	19 (4)	6 (1)	–
Total 2011 (%)	466 (100)	203 (44)	126 (27)	128 (27)	0 (0)	9 (2)	–

Statistics on applications for access under the Freedom of Information Act from 1st January to 31 December 2020

Department		Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
Federal Chancellery FCh	FCh	**21**	12	5	3	0	1	0
	FDPIC	**10**	8		1		1	
	Total	**31**	**20**	**5**	**4**	**0**	**2**	**0**
Federal Departement of Foreign Affairs FDFA	FDFA	**174**	88	14	47	11	4	10
	Total	**174**	**88**	**14**	**47**	**11**	**4**	**10**
Federal Departement of Home Affairs FDHA	GS FDHA	**20**	12	0	5	0	3	0
	FOGE	**4**	3	0	0	1	0	0
	FOC	**3**	1	0	2	0	0	0
	SFA	**3**	1	0	2	0	0	0
	METEO CH	**1**	1	0	0	0	0	0
	NL	**0**	0	0	0	0	0	0
	FOPH	**181**	51	22	69	3	26	10
	FOS	**7**	4	1	0	0	0	2
	FSIO	**19**	15	0	4	0	0	0
	FSVO	**25**	8	3	9	4	0	1
	SNM	**0**	0	0	0	0	0	0
	SWISS MEDIC	**42**	15	0	9	0	10	8
	SUVA	**7**	3	0	0	0	2	2
	Total	**312**	**114**	**26**	**100**	**8**	**41**	**23**
Federal Department of Justice and Police FDJP	GS FDJP	**5**	4	0	0	0	0	1
	FOJ	**29**	18	7	2	0	0	2
	FEDPOL	**13**	6	2	2	1	0	2
	METAS	**2**	2	0	0	0	0	0
	SEM	**19**	10	1	5	0	3	0
	PTSS	**1**	0	1	0	0	0	0
	SIR	**5**	3	0	0	0	0	2
	IPI	**2**	2	0	0	0	0	0
	FGB	**0**	0	0	0	0	0	0
	ESchK	**0**	0	0	0	0	0	0
	FAOA	**1**	0	0	0	1	0	0
	ISC	**0**	0	0	0	0	0	0
	NKVF	**0**	0	0	0	0	0	0
	Total	**77**	**45**	**11**	**9**	**2**	**3**	**7**

	Department/ Office	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
Federal Department of Defence, Civil Protection and Sport DDPS	GS DDPS	**20**	7	0	10	1	0	2
	Defence/Army	**34**	13	0	9	2	9	1
	FIS	**18**	3	8	3	2	0	2
	armasuisse	**12**	9	0	2	0	1	0
	FOSPO	**150**	147	2	1	0	0	0
	FOCP	**17**	5	0	12	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OA	**0**	0	0	0	0	0	0
	Total	**251**	**184**	**10**	**37**	**5**	**10**	**5**
Federal Departmemt of Finance FDF	GS FDF	**22**	11	1	9	0	1	0
	FITSU	**1**	0	0	1	0	0	0
	FFA	**10**	1	1	7	1	0	0
	FOPER	**1**	1	0	0	0	0	0
	FTA	**10**	7	0	3	0	0	0
	FCA	**37**	15	7	5	1	3	6
	FOBL	**3**	1	1	1	0	0	0
	FOITT	**4**	2	0	0	1	0	1
	SFAO	**8**	3	3	1	0	0	1
	SIF	**3**	0	0	1	0	2	0
	PUBLICA	**0**	0	0	0	0	0	0
	CCO	**10**	10	0	0	0	0	0
	Total	**109**	**51**	**13**	**28**	**3**	**6**	**8**
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	**9**	6	1	0	1	0	1
	SECO	**35**	16	10	7	1	0	1
	SERI	**4**	3	0	0	0	0	1
	FOAG	**14**	3	0	7	0	3	1
	FONES	**7**	3	0	3	0	0	1
	FHO	**3**	0	0	3	0	0	0
	PUE	**2**	1	0	1	0	0	0
	COMCO	**18**	11	1	3	1	2	0
	ZIVI	**0**	0	0	0	0	0	0
	FCAB	**2**	2	0	0	0	0	0
	SNSF	**2**	1	0	0	0	1	0
	SFIVET	**1**	0	0	0	0	1	0
	ETH Board	**16**	3	3	10	0	0	0
	Innosuisse	**2**	0	0	2	0	0	0
	Total	**115**	**49**	**15**	**36**	**3**	**7**	**5**

	Department/ Office	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	**9**	8	0	1	0	0	0
	FOT	**14**	9	0	3	2	0	0
	FOCA	**9**	3	0	2	0	1	3
	SFOE	**4**	3	0	0	0	0	1
	FEDRO	**9**	7	0	2	0	0	0
	OFCOM	**14**	2	2	10	0	0	0
	FOEN	**38**	17	5	13	1	0	2
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	ENSI	**7**	3	1	1	0	2	0
	PostCom	**1**	1	0	0	0	0	0
	ICA	**0**	0	0	0	0	0	0
	Total	**105**	**53**	**8**	**32**	**3**	**3**	**6**
Office of the Attorney General OAG	OAG	**13**	6	1	0	0	4	2
	Total	**13**	**6**	**1**	**0**	**0**	**4**	**2**
Parliamentary Services PS	PS	**6**	0	5	0	0	0	1
	Total	**6**	**0**	**5**	**0**	**0**	**0**	**1**
	Total sum	**1193**	**610**	**108**	**293**	**35**	**80**	**67**

Requests for access 2020 with Corona reference

	Department/ Office	Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
Federal Chancellery FCh	FCh	**6** (100%)	3 (50%)	3 (50%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FDPIC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**6** (100%)	**3** (50%)	**3** (50%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Federal Departement of Foreign Affairs FDFA	FDFA	**13** (100%)	12 (92%)	1 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**13** (100%)	**12** (92%)	**1** (8%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Federal Departement of Home Affairs FDHA	GS FDHA	**17** (10%)	11 (6%)	0 (0%)	3 (2%)	0 (0%)	3 (2%)	0 (0%)
	FOGE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SFA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METEO CH	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	NL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOPH	**134** (77%)	44 (25%)	16 (9%)	53 (31%)	1 (1%)	11 (6%)	9 (5%)
	FOS	**1** (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)
	FSIO	**1** (1%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FSVO	**4** (2%)	3 (2%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SNM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SWISS MEDIC	**16** (9%)	4 (2%)	0 (0%)	0 (0%)	0 (0%)	9 (5%)	3 (2%)
	SUVA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**174** (100%)	**64** (37%)	**17** (10%)	**56** (32%)	**1** (1%)	**23** (13%)	**13** (7%)
Federal Departmemt of Finance FDF	GS FDF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FITSU	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FFA	**9** (36%)	1 (4%)	1 (4%)	6 (24%)	1 (4%)	0 (0%)	0 (0%)
	FOPER	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FTA	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FCA	**11** (44%)	1 (4%)	5 (20%)	3 (12%)	0 (0%)	0 (0%)	2 (8%)
	FOBL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOITT	**3** (12%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)	0 (0%)	0 (0%)
	SFAO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SIF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PUBLICA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	CCO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**6** (11%)	**6** (11%)	**9** (16%)	**2** (4%)	**0** (0%)	**2** (4%)

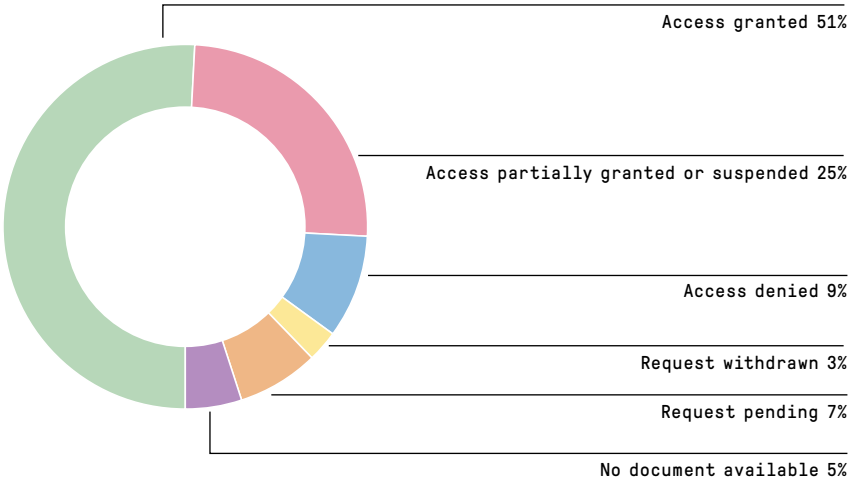
Department/ Office		Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
Federal Department of Justice and Police FDJP	GS FDJP	**1** (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (14%)
	FOJ	**6** (86%)	5 (71%)	1 (14%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FEDPOL	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	METAS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SEM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PTSS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SIR	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	IPI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FGB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ESchK	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FAOA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ISC	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	NKVF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**7** (100%)	**5** (71%)	**1** (14%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (14%)
Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOT	**2** (50%)	1 (25%)	0 (0%)	0 (0%)	1 (25%)	0 (0%)	0 (0%)
	FOCA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SFOE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FEDRO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OFCOM	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOEN	**1** (25%)	1 (25%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ARE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ComCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ENSI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	PostCom	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ICA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**4** (100%)	**3** (75%)	**0** (0%)	**0** (0%)	**1** (25%)	**0** (0%)	**0** (0%)
Federal Department of Defence, Civil Protection and Sport DDPS	GS DDPS	**8** (16%)	1 (2%)	0 (0%)	5 (10%)	0 (0%)	0 (0%)	2 (4%)
	Defence/ Army	**23** (46%)	10 (20%)	0 (0%)	3 (6%)	1 (2%)	8 (16%)	1 (2%)
	FIS	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	armasuisse	**1** (2%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOSPO	**3** (6%)	3 (6%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOCP	**15** (30%)	3 (6%)	0 (0%)	12 (24%)	0 (0%)	0 (0%)	0 (0%)
	swisstopo	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	OA	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**50** (100%)	**18** (36%)	**0** (0%)	**20** (40%)	**1** (2%)	**8** (16%)	**3** (6%)

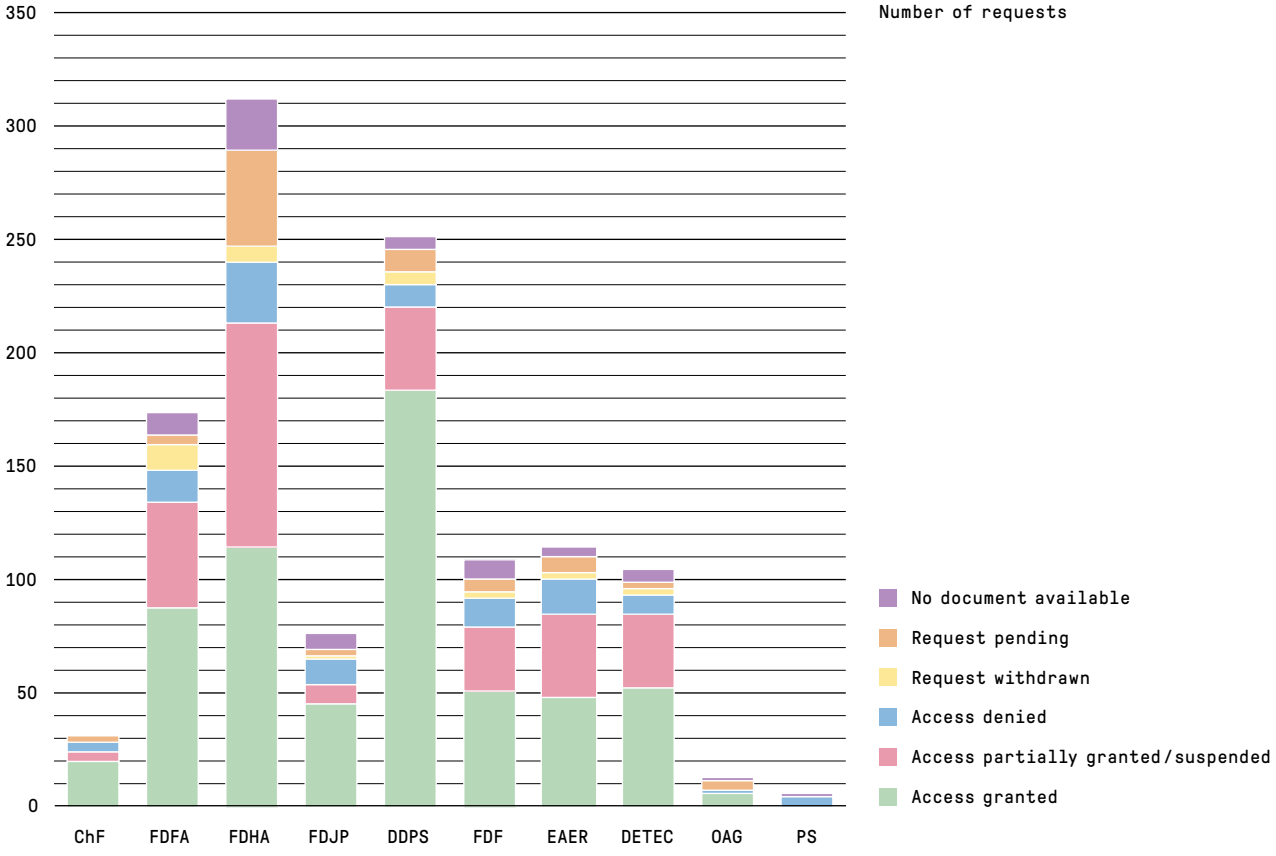
Department/ Office		Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	**2** (8%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SECO	**14** (56%)	5 (20%)	7 (28%)	2 (8%)	0 (0%)	0 (0%)	0 (0%)
	SERI	**1** (4%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FOAG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FONES	**5** (20%)	2 (8%)	0 (0%)	2 (8%)	0 (0%)	0 (0%)	1 (4%)
	FHO	**3** (12%)	0 (0%)	0 (0%)	3 (12%)	0 (0%)	0 (0%)	0 (0%)
	PUE	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	COMCO	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ZIVI	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	FCAB	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SNSF	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	SFIVET	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	ETH Board	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Innosuisse	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**25** (100%)	**10** (40%)	**7** (28%)	**7** (28%)	**0** (0%)	**0** (0%)	**1** (4%)
Office of the Attorney General OAG	OAG	**0** (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Total	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)
Parliamentary Services PS	PS	**4** (100%)	0 (0%)	3 (75%)	0 (0%)	0 (0%)	0 (0%)	1 (25%)
	Total	**4** (100%)	**0** (0%)	**3** (75%)	**0** (0%)	**0** (0%)	**0** (0%)	**1** (25%)

Number of requests for mediation per category of applicants

Category of Applicant	2020
Media	**31**
Privat Persons (or not exact assignment possible)	**42**
Interested parties (associations, organisations, companies, etc.)	**5**
Lawyers	**7**
Companies	**7**
Universities	**1**
Total	**93**

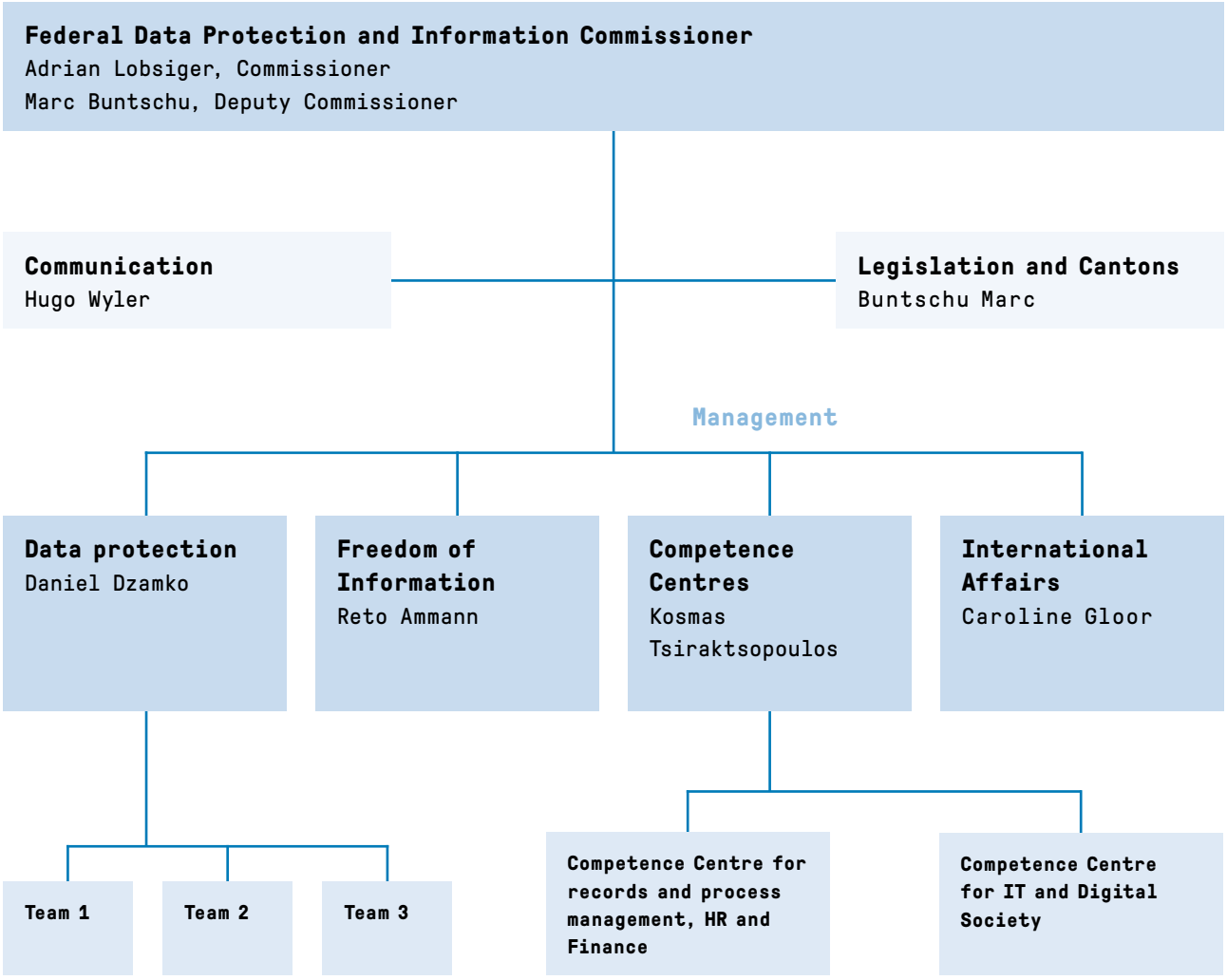
Applications for access in the federal administration from 1st January to 31 December 2020





3.4 Organisation FDPIC (Status 31 March 2021)

Organisation chart



Employees of the FDPIC

Number of employees	38		
FTE	31.8		
per gender	Women	20	53 %
	Men	18	47 %
by employment level	1–89 %	25	63 %
	90–100 %	13	37 %
by language	German	30	79 %
	French	7	18 %
	Italian	1	3 %
by age	20–49 years	24	63 %
	50–65 years	14	37 %
Management	Women	3	33 %
	Men	6	67 %

Abbreviations

AI Artificial Intelligence

BCR Binding Corporate Rules

CJEU Court of Justice of the European Union

Convention 108+ Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

E-ID Act Federal Act on Recognised Electronic Means of Identification

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

EpidA Epidemics Act

EPR Electronic Patient Record

EPRA Federal Act on the Electronic Patient Record

FADP Federal Act on Data Protection

FIS Federal Intelligence Service

FoIA Freedom of Information Act

GDPR General Data Protection Regulation

GPA Global Privacy Assembly

ICT Information and Communication Technology

NaDB national data management programme

NAVS13 13-digit OASI number

NCSC National Cyber Security Centre

PNR Passenger Name Records

Privatim Association of Swiss Commissioners for Data Protection

SCC Standard Contractual Clauses

SDPA Application of the Schengen Acquis in Criminal Matters (SR 235.3)

Figures and tables

Figures

Figure 1: Evaluation of requests for access – trend since 2006 ..... S. 69

Figure 2: Fees charged since the FoIA entered into force ..... S. 71

Figure 3: Mediation requests since the FoIA entered into force ..... S. 72

Tables

Table 1: Amicable outcomes ..... S. 73

Table 2: Processing time of mediation procedures ..... S. 74

Table 3: Pending mediation procedures ..... S. 75

Table 4: Number of employees for FADP concerns ..... S. 82

Table 5: Services in data protection ..... S. 83

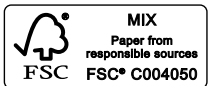
Table 6: Consultancy for large-scale projects in 2021 ..... S. 83

Table 7: Outcome objectives FDPIC ..... S. 85

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. 410.028.ENG

Layout: Ast & Fischer AG, Wabern
Photography: Nicolas Stadler
Characters: Pressura, Documenta
Print: Ast & Fischer AG, Wabern
Paper: PlanoArt®, woodfree bright white



Key figures

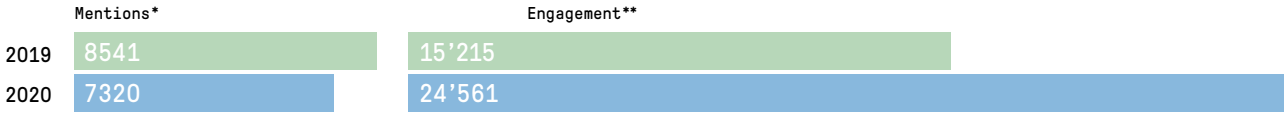
Workload data protection

57,8 %	15,0 %	19,4 %	7,3 %
Consultancy	Supervision	Information	Legislation

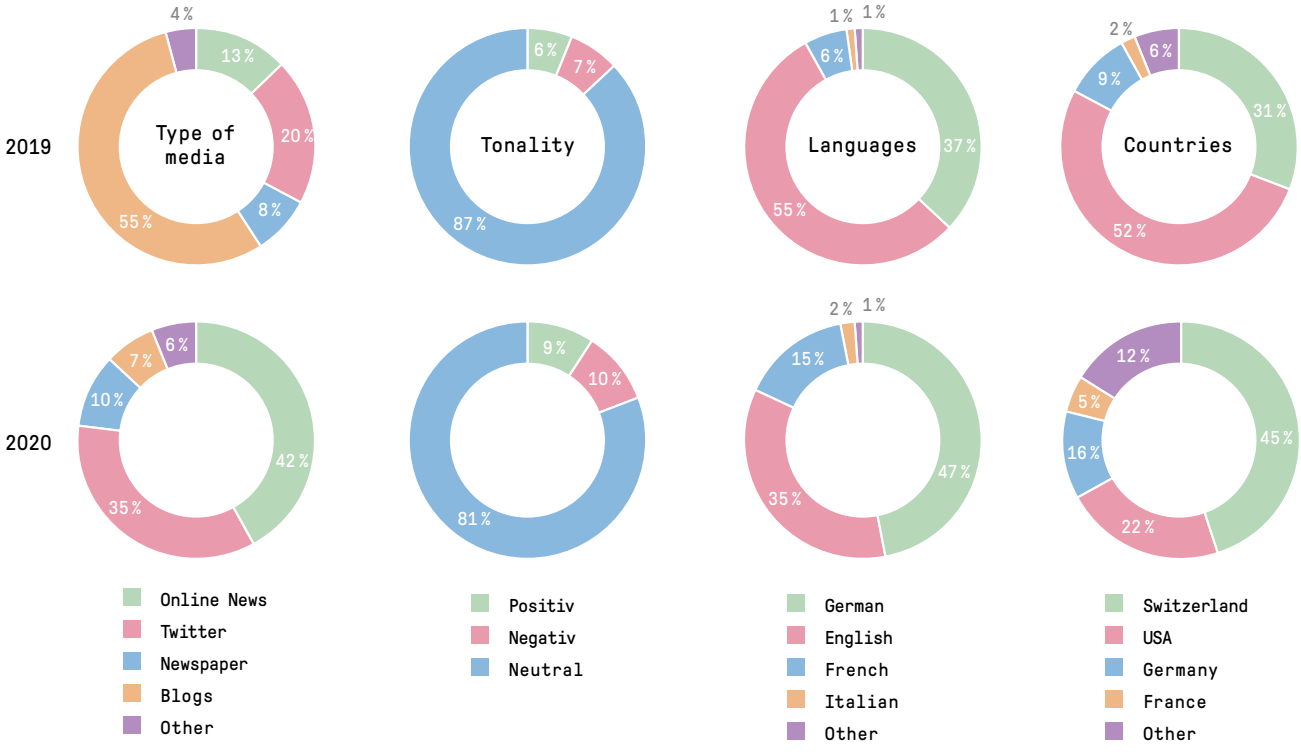
Applications for access Freedom of Information (FoIA)

51 %	25 %	9 %	3 %	7 %	5 %
granted	partially granted or suspended	denied	withdrawn	pending	no document available

Medial resonance of the FDPIC in the Social Web



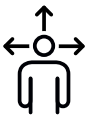
* Number of all mentions of the FDPIC (mentions in Blogs, Twitter, Onlinenews, etc.)
** Number of all interactions (Likes, Retweets, etc.)



Data protection concerns

Fair information

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



Freedom of Choice

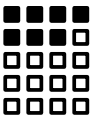
Those affected from data processing (data subjects) give their consent on the basis of transparent information and are provided with genuine freedom of choice.

Risk analysis

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

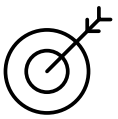
Data correctness

The processing takes place with applicable data.



Proportionality

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



Purpose

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

Data security

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

Documentation

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

Responsibility

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

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

E-Mail: info@edoeb.admin.ch
Website: www.derbeauftragte.ch
@derBeauftragte
Phone: +41 (0)58 462 43 95 (Mo – Fr, 10 am – 12 pm)
Fax: +41 (0)58 465 99 96