





# Annual Report 2019/2020

## of the 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 2019 and 31 March 2020.



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra



## Foreword

It is not digital viruses but natural ones that are dominating the headlines at the end of this reporting period. The coronavirus invades people's living tissues, laying bare our vulnerability as biological beings who have a natural fear of the invisible.

Our digitalised society offers a wealth of services that mitigate our fear of the invisible world of viruses and germs. We place our trust in digital firewalls to protect against computer viruses, while the digital working from home is now proving invaluable against germs. And apps which, by analysing mobility data, create more comfortable travelling conditions with the least possible proximity to other people are helping to protect our health in the preventive sense.

Despite the obvious benefit of digital technologies, despite the justified emphasis on community spirit, discipline and solidarity in a crisis and regardless of our inherent fear of the invisible virus, this is not the time to stop our self-determined thinking. During pandemics and economic crises, it is more important than ever not to let conspiracy theories, superstition or the ruthless striving for power win the upper hand and push us into a trap of a digital guardianship.

At the time of going to print, there is no way of knowing when normality will return. We all hope it will be soon, and with as few casualties as possible. Along with this hope is the expectation that, when this is all over, we will fully regain our informational self-determination – and, in particular, that cash as an anonymous form of payment will survive this crisis even though it sometimes comes with germs attached.

Adrian Lobsiger  
Federal Data Protection and Information Commissioner



Bern, 31 March 2020

<b>Current challenges</b> .....	<b>6</b>
<b>Data protection</b>	
<b>1.1 Digitalisation and fundamental rights</b> ....	<b>14</b>
– Elections and voting: Facebook’s election features	
– Updated guide and new checklist for parties	
– Electronic identity as a tool for maximum protection	
– “SwissID” by SwissSign Group AG	
– De-anonymisation is a risk inherent in AI	
– Federal Statistical Office FSO: Demands for greater transparency and local audits when releasing personal data to other countries	
– Despite elaborate anonymisation, the FDPIC still considers the marketing of mobility data from the mobile phone network to be problematic	
– 5G standard: Sunrise Communications AG taking data protection measures for secure technical implementation	
– Incorrect e-mail addresses at Swisscom	
– Data protection authorities turn their attention to “TikTok”	
– Music streaming service – Personal data requested and analysed by the FDPIC	
– Clearview obtaining facial images without consent	
<b>Focus I</b> .....	<b>24</b>
– Revision of the Federal Act on Data Protection	
– Data Protection Convention 108+ of the Council of Europe	
<b>1.2 Justice, Police, Security</b> .....	<b>27</b>
– DNA profiles: a rigorous legal framework is essential	
– Law on the release of airline passenger data in EU states delayed	
– “Swiss” booking system – Measures being implemented to prevent data misuse	
– Police measures to combat terrorism	
– Technical audit of the use of the Schengen Information System at fedpol and the ISC-FDJP	
– Audit commenced at fedpol relating to the activities of the SIRENE office	
– Schengen Data Protection Act	
– Second review of Privacy Shield	
<b>1.3 Taxation and finance</b> .....	<b>35</b>
– Release of personal data to foreign tax authorities – problematic extension to other states	
– Exchange of Country-by-Country Reports from Multinational Enterprises (CbCRA)	
– The Federal Administrative Court backs the Commissioner’s objection in the FTA case: affected third parties have the right to be informed in advance	
<b>1.4 Commerce and economy</b> .....	<b>37</b>
– Incorrect database entries at collection agency	
– Use of Ricardo data within the Tamedia group (TX Group)	
– Incorrect addresses at Serafe AG – Data accuracy measures needed	
– Transactional data analysis for planning purposes	
– Sporting goods retailer Decathlon provided inadequate information about data procurement	
– Authentication using voice recognition at PostFinance AG	
– Video surveillance using intelligent cameras at Migros	
<b>1.5 Health</b> .....	<b>42</b>
– Dialogue stepped up prior to launch of electronic patient records	
– “Helsana+” bonus programme - Implementation of the Federal Administrative Court ruling	
– “Swiss National Cohort”: additional precautions necessary	
– IQOS: Investigation into the next generation IQOS e-cigarette by Philip Morris	
<b>1.6 Employment</b> .....	<b>45</b>
– Time recording and tracking with apps in the work environment	
– Case investigation into time recording	
– Use of artificial intelligence in the application process	
<b>1.7 Insurance</b> .....	<b>47</b>
– New legal provisions take effect on observations in the social insurance system	
– Draft legislation on the systematic use of the OASI number	
<b>1.8 Traffic and transport</b> .....	<b>49</b>
– New public transport app SmartWay creates personality profiles	
– Audit of a pilot project by SBB and Axon Vibe	
– Protection of privacy in the Mobility Pricing project	
– Cyclomania app by Pro Velo Schweiz	
<b>1.9 International</b> .....	<b>52</b>
– International Conference of Data Protection and Privacy Commissioners ICDPPC in Tirana	
– Conference of European Data Protection Authorities in Tbilisi	
– The Francophone Association of Data Protection Authorities	
– Supervision Coordination Groups on the SIS II, VIS and Eurodac information systems	
– OECD Working Party on ‘Data Governance and Privacy in the Digital Economy’	
– General meetings of the European Data Protection Board (EDPB)	

- European Working Party on Privacy Case Handling
- Sub-Working Group on “Border, Travel & Law Enforcement”
- European General Data Protection Regulation
- Brexit and transfer of personal data
- Consultative Committee on Convention 108 (T-PD)
- Adequacy decision on Switzerland’s level of data protection

#### Focus II ..... 60

- Libra Project
- International activities and meetings

## Freedom of information

2.1	<b>General</b> .....	64
2.2	<b>Requests for access – further increase in 2019</b> .....	65
2.3	<b>Mediation procedure – significant rise in mediation requests</b> .....	68
	– Duration of mediation procedures	
	– Proportion of amicable outcomes	
	– Number of pending cases	
2.4	<b>Office consultations</b> .....	71
	– Office consultations on the draft of a law on customs and border security; opening of the consultation process	
	– Consultations on the agreement between the Confederation and the cantons concerning the harmonisation and sharing of police technology and IT systems	
	– Office consultation on a single point of orientation for official documents	
	– Office consultation on the CAR-T cell therapy charging arrangement	
	– Office consultation on the consultative process for the partial amendment of the HIA regarding cost-containing measures – Package 2	
	– Office consultation on the complete revision of the Ordinance on Public Procurement	

## The FDPIC

3.1	<b>Duties and resources</b> .....	80
	– The Commissioner	
	– Services and resources in the field of data protection	
	– Services and resources in the field of freedom of information	
3.2	<b>Communication</b> .....	84
	– Expansion due to additional tasks and lack of critical mass	
	– Extensive media coverage, at home and abroad	
	– Federal and cantonal data protection authorities joined forces for International Data Privacy Day	
	– Opinions, recommendations and publications	
	– Website still the key channel for our communication	
3.3	<b>Statistics</b> .....	88
	– Statistics on FDPIC’s activities from 1 <sup>st</sup> April 2019 to 31 March 2020 (Data protection)	
	– Overview of applications from 1 <sup>st</sup> January to 31 December 2019	
	– Statistics on applications for access under the Freedom FoIA from 1 <sup>st</sup> January to 31 December 2019	
	– Number of requests for mediation by categories of applicants	
	– Number of requests of the whole Federal Administration	
3.4	<b>Organisation</b> .....	95
	– Organisation chart	
	– Staff	
	<b>Abbreviations</b> .....	98
	<b>Figures and tables</b> .....	99
	<b>Impressum</b> .....	100

#### In the cover

- Key figures
- Data protection concerns

## Current challenges

### I Digitalisation

The corona crisis and the shift it has triggered – from going out to work or shop, to working or shopping from home – is a stark illustration of how critical ICT and the Internet have become to the everyday lives of the Swiss public.

#### Technology and economy

The technical and economic potential for interference in the public's privacy and rights to self-determination remains great.

The Commissioner noted with concern during the reporting period that a growing number of private companies have transitioned to the automated processing of large quantities of biometric data. In some cases, those private companies obtain such data in direct contact with their customers, such as when the latter use voice identification (see chapter 1.4). The Internet is another source from which private companies obtain huge quantities of biometric data, perhaps by trawling social networks for facial images, then processing the copied images using facial recognition software and enhancing them with additional personal data (see article on Clearview in chapter 1.1). Whilst the security services of authoritarian states access personal data at will, either directly or via the operators of telecoms services and platforms, the police authorities in western democracies are subject to constraints, albeit of very varied kinds: in the USA, for instance, certain security agencies already pay to use facial recognition services operated by private companies, yet in Switzerland the police authorities must have a legal basis for using automated facial recog-

niton programmes. Such a basis is currently denied them by the federal and cantonal legislators.

Growing willingness abroad to take full advantage of the improved digital opportunities for monitoring the public has already led to demands for the sharing of image data under the Prüm Convention, to facilitate cooperation between Europe's police forces (see chapter 1.9). The Commissioner expects that, sooner or later, federal and cantonal police agencies will call for politicians to create laws on the widespread police use of facial recognition technology. It is the Commissioner's view that such laws would be problematic. Even if assurances were given that automated comparisons and analyses of facial data would be restricted to particularly serious crimes, there is a risk that, under such laws, the anonymous freedom of movement which people in the public space currently enjoy might become the exception. Experience shows that the thresholds at which crimes are considered by law to have been committed are being gradually lowered: the impact of the related legislation is being undermined by unrelated goals in the areas of security, immigration and administrative law enforcement.

Another cause for concern is the still alarmingly high number in this of complaints during this reporting period about the loss of health data, personnel records, loan applications or photo data, and chat and mail communication. Each time personal data are taken without authorisation or stolen data disseminated, this adds to the mass of openly accessible personal data on the Internet and privacy suffers. Operators of big clouds, which also hold astronomical quantities of private image data, bear a huge responsibility for safeguarding the security of those data with adequate technical and organisational means.



## Society and data policy

As part of the global fight against coronavirus, governments of badly hit regions in Asia, where the virus first emerged, have stepped up their means of digital monitoring of the population – some of which, by western standards, were already very draconian – in order to prevent the further spread of the virus. The arrival of the virus in Switzerland forced the Federal Council to order health policy measures. Having invoked an exceptional situation on 16 March 2020, on the basis of Art. 7 of the Epidemics Act, the Federal Council was able to impose measures which this Act does not describe in detail. The Act requires only that the measures to combat the disease must be “necessary”. In its regularly updated, public comments on the pandemic, the FDPIC repeatedly noted that the use of digital methods to collect and analyse mobility and proximity data in order to prevent infections must be proportionate. In other words, they must be epidemiologically justified and suited to the purpose of containing the spread of the disease at any given stage, and their impact must warrant access to the data subjects’ personal data. On 24 March 2020, the Commissioner appointed a “Corona” task force within the FDPIC to review, from that date onwards, various private and government-run projects to digitally combat the disease. He provides regular updates on the FDPIC website on the work of the task force and the outcomes ([www.edoeb.admin.ch](http://www.edoeb.admin.ch)).

The Commissioner expects that the tragic collective event that is coronavirus will not have the effect of permanently restricting the rights of the Swiss public to informational self-determination and privacy. In his comment, he sounded the precautionary note that personal data processed in order to combat the virus must be erased or anonymised once the pandemic is over.

## Legislation

The legislative work on the complete revision is at an advanced stage. Although the bill has been examined by both Councils, as at the end of the reporting period the outstanding issues had yet to be resolved, the delays having been further exacerbated by the pandemic. The Commissioner hopes that, despite the coronavirus, the outstanding issues will soon be settled and the concluding vote can take place during the summer session.

*“Coping with the pandemic must not result in permanent impairment of free and self-determined life.”*

## II Consultancy and supervision

The FDPIC, in its role as a supervisory body, aims to ensure that the rate of personal data processing is not purely driven by technical feasibility, but is instead subject to legal restrictions. It 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 state data protection authorities. Given this context, we have continued to support many big data projects run by federal authorities and private companies over the course of this reporting period.

Not least in order that he can make effective use of his own resources, the Commissioner continues to encourage parties involved in major projects which pose serious privacy risks to make use on their own initiative of modern working tools, such as privacy impact assessments. In some cases, the Commissioner also encourages companies to set up their own data protection bodies. Over the reporting year, the cost of consultancy services for private projects declined somewhat as a proportion of our complete expenditure.

In December 2018, in partnership with the cantonal data protection authorities, the FDPIC published a guide to the application of privacy law to the digital processing of personal data in the context of elections and voting ([www.edoeb.admin.ch/elections](http://www.edoeb.admin.ch/elections)). This was a particular focus of the FDPIC's consultancy, with a view to the Federal re-elections in the autumn of 2019. In the final phase of the election campaign, the FDPIC published an updated guide for data protection authorities and a checklist that received a lot of media coverage, calling on the political parties to upgrade their websites.

Another priority in consultancy for the transport industry was the design of ticketing apps (see chapter 1.8). The processing of mobility data is providing a particularly sensitive topic, as it lends itself to the creation of personal profiles which are extremely complex to pseudonymise or anonymise (see chapter 1.1). Given this context, it is pleasing that the Council of States recognises that the special protection for profile-building processing, which is lost under the revised FADP, must be maintained and enshrined under the new concept of profiling. The hope is that the two chambers can at least agree on the need to maintain the current level of protection afforded by the current FADP (see Focus I).

After declining significantly in the 2015/16 period, expenditure on supervisory duties climbed again in both the previous and the current period. However, it remains well below the long-term average for previous periods. Since the FDPIC has been continuously under-resourced, this increase required cuts to other services. In this reporting period, the FDPIC was again unable to meet justified public expectations sufficiently with regard to supervision of personal data processing via consumer apps and social networks (see chapter 3.1).

As operational data protection when providing supervisory support for major digital projects is an obvious lead-in to official data protection, the Commissioner and his deputy continued their regular, face-to-face technical discussions with the associations of data protection consultants at private companies in German and French-speaking Switzerland during this reporting period. These discussions were well-attended and proved to be of great practical benefit to everyone involved.

*“Corporate data protection builds important bridges to official data protection in the supervisory monitoring of large-scale digital projects.”*

### III National and international cooperation

#### National cooperation

The FDPIC has continued to cooperate even more closely with cantonal data protection agencies. Some examples of this are: Technical discussions with the cantonal data protection commissioners regarding the introduction of electronic patient records (see chapter 1.5), the joint communication by the federal and cantonal data protection authorities on International Data Privacy Day concerning privacy risks in private and public transport (see chapter 3.2), participation in the various meetings of the Bureau and general meetings of the Conference of Swiss Data Protection Commissioners (Privatim), and meetings of the French-speaking data protection commissioners. These were an opportunity to discuss views on current consultation processes and share experiences in the respective consultancy and supervisory spheres.

#### Signature of Convention 108+

Following a decision of the Federal Council, on 21 November 2019 Switzerland formally signed Convention 108+ in Strasbourg. The Federal Council submitted its dispatch concerning the approval of the protocol to the Swiss parliament on 6 December 2019. By acceding to the modernised convention, Switzerland is seeking to safeguard a high level of privacy protection and to facilitate cross-border data movements in the public and private sector. Accession to the convention is highly relevant to the European Commission's evaluation, which is nearly concluded (see below).

#### New European data protection law

The EU's General Data Protection Regulation (GDPR) has been in force since May 2018. The FDPIC is monitoring its application in the various countries of Europe very closely, and is continually updating its factsheet which was first published in autumn 2017. We remain committed to advising and providing practical support for Swiss companies affected.

*“Work and consumer behaviour are shifting from outside to home.”*

## Evaluation of level of data protection

The European Commission reviews the level of data protection in third countries. It last confirmed Switzerland's adequate level of data protection in 2000. This means that companies in the EU can share personal data with companies in Switzerland without taking additional measures. The EU's evaluation process on the basis of the GDPR officially commenced in March 2019. Over the course of the reporting year, the FDPIC shared his expertise with the working party led by the Federal Office of Justice (see chapter 1.9). The Commission's report on the process is expected at the end of May 2020.

Having voted in the June 2016 referendum to leave the EU (Brexit), the UK's departure happened on 1 February 2020. The FDPIC attended numerous meetings with authorities of the Confederation and the UK to make sure that the free movement of personal data between Switzerland and the UK can continue post-Brexit. The UK is considered to afford an adequate level of protection, and the FDPIC currently sees no cause to alter that status. The EU will decide by the end of 2020 whether it still deems the UK to offer an adequate level of data protection. The FDPIC continues to actively monitor developments (see chapter 1.9).

## Swiss-US Privacy Shield

In the autumn of 2019, as part of a delegation led by Seco, we undertook the second supervisory review of the Swiss-US Privacy Shield. Although the review again identified weaknesses, overall the functioning of the Privacy Shield had further improved (see chapter 1.9).

The highly anticipated ruling in the legal case that is currently pending before the Court of Justice of the European Union (CJEU) regarding the transfer of data from the EU to the USA (Schrems II), during which the EU-US Privacy Shield Framework may also come under scrutiny, is still not forthcoming. The ruling will not directly affect Switzerland. Once a decision has been announced, the FDPIC will analyse its potential relevance to the Swiss-US Privacy Shield Framework.

*“Companies in the EU can exchange personal data with companies in Switzerland without further measures.”*





# Data protection

## 1.1 Digitalisation and fundamental rights

### Elections and voting: Facebook's election features

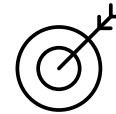
During the Federal elections in 2019, Facebook used features to target voters on its social media platform. The company confirmed to the FDPIC that it was complying with the data protection requirements laid out in the guide on elections and voting.

Having been alerted by media reports that Facebook may be planning to use election features such as the “voter button” on its social media platform in the run-up to the Federal elections in 2019, the Commissioner wrote to the company's designated contact points, requesting comment. In his letter, the FDPIC referred to his guide on elections and voting (see box) and pointed out that operators of social networks must provide fair and complete information about the digital processing methods used in connection with elections.

Such transparency is essential in order for the voting public to assess whether, and how, their opinions or their voting behaviour is being influenced.

In response, Facebook Ireland Ltd. wrote to the FDPIC to confirm that the platform would be using these functions one day prior to the elections, and on election day. It said that, on the election date, the social network would be reminding all Facebook users in Switzerland aged 18 and over, without exception, about the election. The company also assured us that Facebook would not be targeting this reminder at specific groups or individuals.

According to the written assurances, the sole purpose of the features was to raise users' awareness of the upcoming



elections and encourage participation – for example, by enabling the individuals concerned to post to their profile telling people they had voted.

Facebook stressed that the political views of the users concerned would not be processed when they did this. Furthermore, Facebook stated that the company would observe the transparency requirements laid down in our guide. Data subjects must have access to multi-level information, via hyperlinks, about the functions and methods used and their processing bases. The FDPIC informed the public of Facebook's assurances via his website.

### Updated guide and new checklist for parties

**Before the final phase of the 2019 Federal elections, the FDPIC published an updated guide for data protection authorities and a checklist that received a lot of media coverage, calling on the political parties to upgrade their websites.**

At the end of 2018, the federal and cantonal data protection authorities published guidelines on the processing of personal data in connection with elections and voting. The aim was to exhort the political parties and other parties, such as operators of social networks or data traders, to process data relating to the federal elections in a privacy-compliant manner. In particular, the guidelines explain to political parties how they can achieve the fundamental data protection principle of transparency with regard to voters' justified expectations. (see 26<sup>th</sup> Annual Report, chapter 1.1).



Prior to the final phase of the election campaign, the FDPIC updated the guidelines and added a checklist for the political parties. This checklist contained control questions which attracted a lot of media coverage, prompting a number of parties to upgrade their websites ahead of the election date in a bid to fully comply with the Data Protection Act.



After the election features went live, the Commissioner reviewed the implementation of the transparency requirements and found that Facebook was informing users about the associated data processing actions in the described manner. He was also satisfied that all further activities, such as posting by specific individuals about vote participation, was undertaken independently and voluntarily by users. As there were no indications of other privacy-related shortcomings, he did not have to take further measures. Even after the 2019 elections, we continue underlining the importance of upholding privacy in the political context. We will continue supervising the situation in Switzerland in this regard.

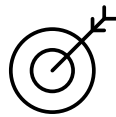


## Electronic identity as a tool for maximum protection

The Federal Act on Recognised Electronic Means of Identification (E-ID Act, BGEID) established a legal basis for the secure identification of individuals in online commerce or in e-government applications. The FDPIC was able to successfully present his concerns during the legislative process.

The division of tasks between the government and private companies remained a politically contentious issue during the now completed parliamentary consultations on the E-ID Act. As “Identity Providers” (IdP), under the standardised legal framework of the E-ID private companies can be authorised to issue electronic identities, provided they have been officially accredited by an independent commission, EIDCOM. EIDCOM accredits private applicants who offer a guarantee that they satisfy the technical and security-related requirements of the E-ID Act. Accredited IdPs are subject to ongoing supervision by EIDCOM. Before recognising an IdP, EIDCOM seeks the input of the FDPIC concerning data protection regulations.

While the bill was being prepared by the administration, and during the consultations on the Federal Assembly’s Legal Affairs Committees, the Commissioner argued that the E-ID Act must make access to the Internet and the use of e-commerce contingent upon the provision of a secure ID. We also ensured that IdPs are not permitted to share any data with third parties for commercial or similar purposes. Data may only be dis-



closed to an online service provider when necessary so that the provider can identify the person concerned in order to fulfil contractual obligations, and provided the user has been informed before the data are first shared.

Such disclosure of data must be the subject of an agreement between the IdP and the online service provider, and must also be submitted to the FDPIC for review. Since our concerns were taken into account when the legislation was drafted, the Commissioner considers that the E-ID Act complies with the Confederation’s data protection legislation.

The National Council and the Council of States adopted the E-ID Act during the concluding votes on 27 September 2019. The Act is now being challenged by a referendum which seeks to place the issue of electronic identities entirely in government hands.

### “SwissID” by SwissSign Group AG

**SwissSign Group AG’s “SwissID” product has systemic relevance. As a consultant supervisory body, the FDPIC is overseeing the company’s projects.**

SwissID”, by SwissSign Group AG, is a product for online commerce which entails both pure single sign-on (SSO) services and the issue of an electronic identity (see the main text) on a private basis. With a view to the imminent E-ID Act, the product is to be expanded to enable users to complete online – using a government-recognised electronic identity – those legal transactions for which identity verification is required in order to procure government services on the Internet.

After SwissSign Group AG set up an internal data protection office and tasked it with analysing the privacy risks, during the year under review the FDPIC attended regular meetings with the project managers and began by insisting that anonymous registration must be possible for pure SSO services. Customers must be able to log in with details they have provided themselves, and must not be subject to either a duty of truthfulness or an identification procedure.

Furthermore, the company must ensure that personal data identifying the user are only shared with the online service provider if the latter absolutely needs the data in order to complete its legal transaction. It must not be possible to circumvent this principle by asking the user for additional consents.

SwissSign Group AG has assured the FDPIC that it will incorporate these principles in its data policy and that it will implement them in contracts with online service providers and “SwissID” users.

## De-anonymisation is a risk inherent in AI

Working with the FDPIC, a Federal Working Group has drafted data protection requirements for artificial intelligence (AI). One of the risks of AI systems is the potential for personal information to be deduced from a combination of non-personal data.

In connection with the revised “Digital Switzerland” strategy, the Federal Council decided to establish an inter-departmental working group on artificial intelligence (AI). Separate project groups were tasked with individual aspects of AI. The FDPIC was involved in the project group on data availability/data use and legal parameters/legal certainty.

The full report states that, using a combination of non-personal data elements filtered out of huge volumes of data (big data), AI systems are capable of deducing information which enables individuals to be traced and their identity established (“de-anonymisation”). The report was acknowledged by the Federal Council in December 2019 and published by the State Secretariat for Education, Research and Innovation SERI.

## Federal Statistical Office FSO: Demands for greater transparency and local audits when releasing personal data to other countries

Recently, the Federal Statistical Office (FSO) has begun using a provider for scanning services which undertakes some aspects of the contractually assured service abroad. As regards the associated release of personal data to other countries, the FDPIC deems that the contractually agreed measures to protect personal data abroad offer an adequate level of data protection. However, he is calling for more transparency for data subjects and local audits of the data processor.

Due to the cessation of digitalisation and scanning services at the Federal Office of Information Technology, Systems and Telecommunication at the end of 2018, the Federal Statistical Office, together with the Federal Office for Buildings and Logistics, was tasked in a WTO process with evaluating a new provider of scanning services. Once the WTO process was complete, “Tessi document solutions GmbH” was awarded the contract. The paper documents involved are scanned in Geneva, where they are then either securely destroyed or returned to the FSO. Consequently, the paper questionnaires do not leave Switzerland.

After being scanned, text fields (sections of documents) that are identified as incorrect are manually corrected abroad. The electronic processing solution used for this only shows the user abroad the image of the text fields for correction; the full documents remain on systems in Switzer-

land. Consequently, this is an instance of cross-border disclosure of data, pursuant to Art. 6 FADP. The FSO has shared with the FDPIC extensive documentation, as well as the relevant contractual agreements, which demonstrate that significant technical, organisational and contractual measures are in place to protect personal data abroad. The FDPIC noted that, as the instructing party, the FSO is responsible for data protection and for data security along the entire processing chain and, in accordance with Art. 10a, para. 2 FADP, must also ensure that the third party safeguards data protection and data security. Given the scope of this project, the FDPIC also deemed it advisable to carry out random inspections of the premises where data are processed.



Furthermore, to uphold the privacy-related principle of transparency, the Commissioner considers it essential that the FSO

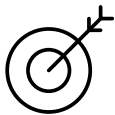
actively informs data subjects of the full circumstances of disclosure of data abroad. In the Commissioner’s view, data subjects must be informed by means of a corresponding note on the FSO’s survey questionnaires.

Privacy considerations must already be taken into account very early, during the WTO evaluation phase of projects involving the processing of personal data. The FDPIC will continue monitoring the project and reviewing the implementation of the measures demanded.

**Despite elaborate anonymisation, the FDPIC still considers the marketing of mobility data from the mobile phone network to be problematic**

People’s movement habits are unique. Therefore, even after deploying sophisticated anonymisation methods, it is impossible to entirely prevent individual people being identified with relative ease, based on this clear movement pattern and additional information. Therefore, the data must be classed as personal data, requiring the data subjects’ consent in order to be processed, and must be protected accordingly.

Mobility data from the mobile phone network are still widely used by businesses for statistical purposes. Today, data processors can use mobility data to determine the exact location of people on foot, and the routes along which they are driving, flying, or using public transport. The mobility data are used for various purposes, such as improving traffic flows or planning the ideal location for a store.



In 2019, the FDPIC received an enquiry from a company concerning the use of such data. The question was whether, after using an “anonymisation method” described in great detail in the documentation, data of mobile phone providers that are classed as “personal data” can be shared with the company. The method involves several anonymisation steps by the mobile phone provider, so that only the statistical patterns of individuals’ behaviour are shared with the company. Among other things, this means that precise information on the locations of mobile devices is not recorded. However, these imprecise location data can be used to calculate possible mobility patterns, and the most likely pattern can then be selected. This results in mobility profiles which, whilst they reflect the patterns of the real-world population, are not intended to depict an individual’s actual behaviour.

In the FDPIC’s estimation, the “anonymisation method” used substantially reduces the potential to re-identify individuals. However, there is still a chance that the shared data and aggregated place of residence and place of work could be used to trace an actual individual. Rural regions with low population densities are particularly susceptible. However, experience suggests that re-identification is not such a complex task as to dissuade an interested party from attempting it. Therefore, there is always a possibility that, in isolated cases at least, the available data and additional information could be used to identify an individual with relative ease; consequently, the data constitute personal data pursuant to Art. 3(A) FAPD.

In such an event, personal data recorded for the purposes of providing and billing mobile phone services can be used for other purposes. As a consequence of this change of processing purpose, the data subjects’ consent must be obtained and measures must be taken to protect personal data.



### **5G standard: Sunrise Communications AG taking data protection measures for secure technical implementation**

The FDPIC undertook technical investigations into the privacy-compliant implementation of the new 5G telecommunication standard. The investigations found that Sunrise has taken state-of-the-art technical and organisational measures to minimise risk.

The new 5G telecommunication standard, which is the successor to the current 4G/LTE standard, promises not just more bandwidth and the ability to have more devices connected at the same time, but also data transmission in near-real time. Thus the 5G telecommunication standard forms the basis for a multitude of future applications, from IoT (Internet of Things) sensors in industry to connected cars or self-driving vehicles. Although 5G is an international standard for mobile Internet and mobile telephony, its implementation by individual providers varies greatly. Moreover, public reports by researchers at ETH Zurich [arXiv:1806.10360v3 [cs.CR] 18 Oct 2018] and the Universities of Purdue and Iowa [NDSS '19, 24-27 February 2019, San Diego, CA, USA Copyright 2019 Internet Society, ISBN 1-891562-55-X] identify security gaps in the new 5G standard (including in the paging protocol, with ToRPEDO and PIERCER attacks). That said, the reports find that, overall, the new standard is more secure than the previous 4G standard.

Having been given the complete documents on the implementation approach chosen by Sunrise Communications AG, the FDPIC was able to form a detailed impression of the security level and of the measures taken. We found that adequate and proactive measures are in place to tackle the security risks, in line with the latest international standards, and the necessary steps have either been planned or already taken. The changes to existing services necessitated by 5G have been subjected to external security assessments, and the requisite technical and organisational measures have been taken to minimise risk.

### **Incorrect e-mail addresses at Swisscom**

A data breach in one of Swisscom's customer systems resulted in e-mails being sent to the wrong addresses. The company swiftly took appropriate action.

The FDPIC learned from a report by a member of the public that a customer of Swisscom had received a large number of e-mails that were not intended for him. The FDPIC asked Swisscom to comment. The company explained that it was already aware of the problem, and had instructed a task force to carry out a risk analysis. Apparently, it was discovered that generically entered e-mail addresses in one of Swisscom's customer systems were not assigned to the right customers. As a result, some Swisscom e-mails were sent to a third-party account. Once the incident came to light, Swisscom deleted the e-mails from the unintended recipient's system.

According to information from Swisscom, it has since identified the wrongly-assigned e-mail addresses and taken immediate action to prevent any further e-mails from Swisscom being sent. Moreover, according to the company there are no indications that the incorrectly addressed e-mails have been misused. The company is now adapting its processes to prevent such occurrences in future.



The FDPIC took note of the immediate measures based on Swisscom's risk analysis. As Swisscom had taken instant action, he did not need to make any further recommendations.

### **Data protection authorities turn their attention to "TikTok"**

Video platform TikTok is hugely popular with children and young people. The FDPIC contacted the app's Chinese operator, as the terms of use for Swiss customers are unclear. He is also in contact with the British data protection authority ICO to clarify questions surrounding users' privacy.

"TikTok" is a video platform that is particularly popular with young people, and download rates for the app are skyrocketing in all app stores. "TikTok" enables users to upload self-produced video clips with a variety of effects and filters, and share them with other users. The platform's social media functions make it very easy to contact other users, react to their videos, and comment on them.

The app is owned by Chinese Internet technology company Bytedance, which has its head office in Beijing. Various misgivings and criticisms are being voiced against the video portal's owner in the media, with accusations that it is failing to protect children's privacy, censoring or filtering certain content in line with Chinese rules, and more besides.

The FDPIC found that it is not clear to Swiss users which terms of use apply to them, as the terms refer to the EU area. He asked the appropriate office at “TikTok” to comment on this question and on the measures to protect children and young people. In addition, he demanded that the company name a designated contact who can provide expert information on matters of data protection.

The company commented on the questions and named a contact. The FDPIC is in contact with the British data protection authority ICO which, during the year under review, opened an investigation into TikTok’s approach to protecting children and young people and the handling of their data.



### Music streaming service – Personal data requested and analysed by the FDPIC

A music streaming service requested access to its users' GPS data in order to check home addresses. During its investigations, the FDPIC issued an information request and subjected the data received to a detailed analysis. The investigation was concluded without any formal action.

During the year under review, a number of newspaper reports were published concerning a popular music streaming service. According to these reports, users had recently been asked to verify their location by transferring the GPS data on their smartphone, in order to check that they form part of a particular household for billing purposes. This prompted the FDPIC to review the legality of the data processing, and he submitted an information request to the music streaming service for specific usage data. Our analysis of the data revealed that the provider processes the user data it obtains in accordance with its own terms of use and data protection provisions. In our opinion, the provisions, which we also reviewed, are clearly worded and satisfy the legal requirements. No anomalies were detected in this regard

The user's consent to transferring GPS data to the provider is described as voluntary in the provider's privacy statement. In fact, when prompted, users can choose whether they want to confirm location by GPS signal or by providing a postcode. Since there is no obligation for customers to transfer GPS data to the music streaming service, the FDPIC concludes that there are no grounds for complaint.



The retention period for user data was also reviewed. A distinction is made here between user data and usage data:

- User data are recorded when creating a user account, and contain identity and contact data that are used and retained for as long as the service is used. This information is needed in order to get in touch, and for accurate billing. As regards the GPS data requested by the streaming service to determine location, no such data were found in the user data received. An individual's user data can only be erased by definitively closing the account and, therefore, waiving use of the streaming service. There can be no objection to this procedure, as copyright rules preclude use of the service without registering for the streaming offering.

- The situation as regards usage data is different. These data are created while using the service, and contain information on its usage. Whilst this information improves the user experience, it is not essential for user management. Therefore, usage data can be controlled by the user, who has the ability to delete the data he has generated, such as playlists. Other usage data, such as listening history, are stored for ninety days, then automatically deleted. This procedure is proportionate and does not contravene the legal requirements.

As the FDPIC did not find any evidence of disproportionate measures by the music streaming service, the investigation was concluded without formal action.



## **Clearview obtaining facial images without consent**

The FDPIC has repeatedly issued warnings on his website about the threat presented to individuals' privacy in Switzerland by the practice of obtaining facial images from the Internet without consent.

Media reports claim that the US providers of the Clearview app are operating a database of around three billion facial images, which they obtain by trawling the Internet and social networks. The business model involves Clearview comparing any photos with the database, for its paying customers, and assigning the matches to identifiable individuals based on additional information. Apparently, Clearview's customers include police authorities.

As we must assume that facial images of residents of Switzerland are also processed in Clearview's database, in January 2020 our authority issued a number of comments on the Clearview application on our website. We wrote to Clearview stating that Swiss data protection legislation and the privacy of data subjects in Switzerland would be seriously violated if their facial images were obtained without permission and processed for foreign police authorities. We told the social networks, whose terms of use normally prohibit the unsolicited trawling of their platforms by third parties or their robots, that they must introduce better technology to protect their customers' image data.

Furthermore, we called upon users of social networks to take responsibility for changing their default settings to make photo material inaccessible to search engines.

To assess the extent to which the Swiss public is affected, on 24 January 2020 the Commissioner submitted a request to Clearview for information and for the erasure of the data processed about him. Despite having sent a reminder, no response had been received by the end of the reporting period. The Directorates of the Federal Office of Police (fedpol), the Federal Customs Administration (FCA) and the Federal Intelligence Service (FIS) promptly confirmed to the FDPIC, at his request, that they neither use, nor intend to use, Clearview or similar applications in the context of their activities.

Within his legal remit, the Commissioner will do his utmost to protect the Swiss public against the unsolicited procurement of their facial images, ensuring that they can continue navigating the virtual and physical realm with anonymity.

# Revision of the Federal Act on Data Protection

Last year, the complete revision of the Federal Act of 19 June 1992 on Data Protection (FADP) passed some major milestones. Having been reviewed by the Political Institutions Committee of the National Council, then by its counterpart on the Council of States, the draft has now entered the resolution of differences phase. The extraordinary situation in which we currently find ourselves as a result of the Covid-19 pandemic is hampering the legislative process, and will probably delay the adoption of the revised Act. It will therefore be a while before the Federal Act on Data Protection related to the Application of the Schengen Acquis in Criminal Matters (SDPA), which entered into force on 1 March 2019 on a provisional basis, can be repealed and written into the new FADP.

During his involvement on the Parliamentary committees to which he was invited, the Commissioner recommended adopting adequate measures to deal with dynamic technological advances and the associated risks. He supported the proposals offering Swiss people a level of protection that is equivalent to the Council of European Convention on Data Protection (Convention 108+) and similar to the European General Data Protection

Regulation (GDPR), which is already applied as a best practice by many businesses and entities in Switzerland for the benefit of their Swiss customers. Building on the existing approach to data protection, the draft thus reinforces its fundamental principles, such as privacy by default and by design, which will be in addition to the pre-existing principles. The terminology has also been modernised and aligned with European law, albeit with some differences remaining that are likely to cause a degree of legal uncertainty and present problems in practice. Some of these stem from genuine conceptual differences, such as the definitions of “profiling” and “high risk profiling” introduced by the Council of States which differ greatly from the National Council’s definition.

This reform thus enables Switzerland to keep the commitments it made when it recently signed Convention 108+ and – hopefully – maintain an adequacy decision that will preserve full access to the European markets for Swiss businesses.



## Data Protection Convention 108+ of the Council of Europe

In October 2019 the Federal Council decided to sign the Protocol of Amendment to Convention 108 of the Council of Europe (Convention 108+). Following this, Switzerland formally signed Convention 108+ on 21 November 2019, in Strasbourg. The dispatch concerning the approval of the protocol was issued to the Swiss federal parliament by the Federal Council on 6 December 2019. Switzerland's objective is to safeguard an internationally recognised standard of data protection.

In the 26<sup>th</sup> Annual Report, the FDPIC observed that it would be beneficial for the Federal Council to sign the modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe.

Switzerland ratified the original data protection convention, which entered into force in 1985, on 2 October 1997. To bring it into line with technological advances and the challenges of digitalisation, it has been revised in recent years by the Council of Europe and has been open for signature since October 2018. The Protocol of Amendment has so far been signed by more than 30 countries, and ratified by a few already.

It is very important that Switzerland accedes to the modernised Data Protection Convention of the Council of Europe. The convention strengthens the protection of persons in our country whose personal data are processed in one of the contracting states. Moreover, it simplifies data exchanges between the contracting states, as well as ensuring that cross-border data transmission remains possible without additional hurdles. Furthermore, the Convention will be key during the impending review by the EU of the adequacy of data protection in Switzerland, as the EU also factors a state's endorsement or otherwise of the Convention into its decision.

Convention 108+ extends the obligations of data controllers, requiring them in particular to report certain privacy breaches to the competent supervisory authority. It also reinforces the rights of data subjects as, in certain cases, the data holder must inform the data subject about the acquisition of personal data. Moreover, the data processor must perform a privacy impact assessment prior to undertaking certain types of processing. Privacy by design and privacy by default must be built-in at the project planning stage. The Protocol of Amendment also provides for an extension of data subjects' rights, particularly with regard to their right to information and their right to object to automated decision-making. The contracting states are further required to introduce a system of sanctions and appeals, and to confer upon supervisory authorities the power to enact binding decisions.

The Federal Council decided on 30 October 2019 to sign Convention 108+. Switzerland then formally signed the convention on 21 November 2019, in Strasbourg. Subsequently, at its meeting of 6 December 2019 the Federal Council adopted the dispatch concerning the approval of the Protocol of Amendment to the Data Protection Convention of the Council of Europe to the Swiss parliament, which must decide on its ratification.

Acceding to the modernised convention enables Switzerland to safeguard a high level of privacy protection and facilitate cross-border data movements in the public and private sector, which is also important to the Swiss economy.



Arrival 2

Taxi

Furniture  
Lost & Found 112

Check-in 2

## 1.2 Justice, Police, Security

### DNA profiles: a rigorous legal framework is essential

In the consultation on the draft amendment of the Act on DNA Profiles between the federal offices concerned, the FDPIC essentially welcomed the proposed changes and new provisions. However, he asked that a rigorous legal framework be established for the new instruments (kinship testing and phenotyping).

In the FDJP's draft amendment, provisions based on the Act on DNA Profiles are separate from those based on civil and military criminal procedure codes. The FDPIC welcomed this proposed clarification.

■ ■ ■ ■ ■  
 ■ ■ ■ ■ ■  
 ■ ■ ■ ■ ■  
 ■ ■ ■ ■ ■  
 ■ ■ ■ ■ ■

A new solution for the retention of DNA profiles is also proposed, which takes account of the proportionality principle and the specific requirements of criminal law relating to minors.

As regards kinship testing and phenotyping, the FDPIC is demanding that strict conditions be imposed to guarantee the proportionality of infringements of data subjects' fundamental rights. The FDPIC takes the view that these instruments must be seen as a last resort. They must only be used to investigate serious crimes, depending on the nature of the legal interests affected, such as crimes against life, limb or liberty, or sex offences. However, kinship testing and phenotyping, along with mass testing, must not routinely be employed in the case of theft. Phenotyping does not determine certain features, such as hair colour, with sufficient precision, and this could prove problematic with regard to the principle of data accuracy. When conducting kinship testing, gathering data is a violation of the right to refuse to testify, which can only be justified for the most serious crimes.

As mentioned above, kinship testing and phenotyping must be reserved for the most serious crimes, depending on the nature of the legal interests against which the crime is committed. Given the difficulty of producing an exhaustive list of crimes which warrant such measures, the FDPIC has proposed that this be decided by the compulsory measures court, as is already the case for mass testing.

### Law on the release of airline passenger data in EU states delayed

The FDPIC continued overseeing work to create a legal framework for the release of passenger data by airlines to EU states. On a number of occasions, we reiterated the urgency of creating such a framework as soon as possible.

As the FDPIC stated in the 2018/2019 Annual Report, a number of EU states were planning to demand that airlines release their passenger data for flights from Switzerland. Their basis for doing so is EU Directive 2016/681 of 27 April 2016 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (EU PNR Directive). We pointed out to the competent federal authorities that this necessitates a legal framework. The FDPIC was assured that a revision of the Air Navigation Ordinance would establish a legal basis for the delivery of PNR data to states which demand the data pursuant to the EU PNR Directive (see p. 24 f. 26 Annual Report 2018/19).

As the federal office responsible, the Federal Office of Civil Aviation (FOCA) then set the necessary legislative work in motion. From the outset, the FDPIC advised the FOCA, until the office decided to put its work on hold on the grounds that the work so far had revealed the need to first create a legal framework in a formal act. Furthermore, the FOCA said, a decision is expected imminently by the Federal Council on the next steps as regards the use of passenger data to further

Swiss efforts to combat serious crime and terrorism. In light of this, the FOCA argued, it makes sense to combine the two bills and deal with them simultaneously.

The FDPIC reiterated the urgent need to create a legal framework. Without such a framework, the release of PNR data by airlines to authorities in the EU would be unlawful. For the sake of completeness, we also noted that agreements must be finalised allowing airlines to release PNR data to third states (i.e. outside the scope of application of the EU PNR Directive). Subsequently, the Federal Office of

Police, fedpol, began work on the legal aspects of the use of passenger data to help Switzerland combat serious crime and terrorism, including the release of passenger data to EU states pursuant to the EU PNR Directive. The FDPIC also commented on this, as part of the office consultation, and maintained his previous stance. In February 2020, the Federal Council announced that, in principle, it was in favour of using passenger data in Switzerland to combat terrorism and crime. The FDPIC will continue overseeing the legislative work in an advisory capacity.



### **‘Swiss’ booking system – Measures being implemented to prevent data misuse**

In the last activity report, the FDPIC reported on the booking system of the airline Swiss. The company promised that certain changes, including partially obscuring the passport number, would be implemented when it launches its new website. However, the launch was delayed.

As mentioned in the last Annual Report, in response to the Commissioner’s request airline company Swiss revised its General Conditions of Carriage to make its customers more aware of the importance of protecting personal data that are visible/stored on the boarding pass. Furthermore, the passport number which, in certain cases, is visible when the booking is



retrieved, was to be partially obscured. (see 26<sup>th</sup> Annual Report, chapter 1.2). Swiss told the FDPIC that the changes would be made

when its new website went live. However, the switch to the new website architecture and, with it, the hiding of the passport number were delayed. Therefore, in a separate move, Swiss decided to begin hiding passport numbers as well as Visa/Green Card data on its website before the new website launch by leaving the first two characters of passport numbers and Visa/Green Card data legible when the booking is retrieved and replacing all subsequent characters with an “x”. Swiss made this change at the end of 2019.

### **Police measures to combat terrorism**

From the FDPIC’s point of view, the enactment of police legislation at federal level is an essential prerequisite for the drafting of new rules. The FDPIC thus raises doubts about all the proposed police measures to combat terrorism drafted so far.

In its annual reports for the last several years, the FDPIC has criticised the fact that the rules governing police activities on behalf of the federal government are governed by a range of different decrees. In contrast to the cantons, there is no “police act” comprehensively governing duties, powers and the processing of personal data. The Federal Office of Police is responsible for a large number of databases. This would facilitate the centralised processing of data for which protection is extremely important and in relation to which exchanges take place between the police authorities of the federal government and the cantons as well as with other countries.

The data are processed on the basis of a plethora of special police-related laws, the handling of which is full of difficulties even for specialised legal experts (not to mention police personnel on the ground). As a result, even investigations regarding the processing of data have long been coming up against their limits in light of this complexity. Instead of drafting a law governing the duties of the police or at least a law on information and cooperation at the federal level, the Federal Department of Justice and Police (FDJP) is constantly having to formulate new provisions, e.g. on police measures to combat terrorism or on explosives precursors. This makes the already intolerably complex rules even more cumbersome, while certain questions remain unanswered. In which systems should retained data be processed, and in what way and over what period of time?

Given this state of affairs, the FDPIC is no longer willing to support legislative projects in sensitive areas – e.g. regarding police measures to combat terrorism – in the parliamentary phase. The FDPIC calls the whole of the FDJP’s draft fundamentally into question. Despite the criticism we published in our last annual report (see 26<sup>th</sup> Annual Report, chapter 1.2), which was also published in the media, the advisory commission of the Council of States (where the matter was first debated) declined to consult the FDPIC on this matter.

### **Technical audit of the use of the Schengen Information System at fedpol and the ISC-FDJP**

As the supervisory authority for the “Schengen Information System” (SIS), the FDPIC has carried out a technical audit at fedpol and the ISC-FDJP. The report is currently being revised.

The N-SIS is the Swiss national version of the central SIS (C-SIS). The processing of data in the N-SIS, and the transmission of data to the central SIS, are described in the “N-SIS Information System and its Subsystems” processing regulations. In Switzerland, more than 30 000 users of various federal (e.g. RIPOL, SEM), cantonal (e.g. cantonal administrations and police) and municipal bodies use the N-SIS.

The ISC-FDJP develops the system and supplies the service to fedpol, which manages it. We carried out this technical audit at both bodies. Other bodies, such as RIPOL, ZEMIS and the cantonal police, were contacted as part of the review, but were not themselves audited.

The primary objective of this audit is to ensure that state-of-the-art technical and organisational measures are in place to secure and protect data stored and used in the system. These measures are based chiefly on ISO 27001. The second objective is to check that these measures are being implemented.

Based on discussions about our list of questions and the aspects audited, we decided to look in greater depth at some specific points. The evaluation of the control had not yet been completed at the end of the reporting period.





Check-In 3



Zuschauerterrasse  
Observation Deck

11.00  
18.55  
11.00  
18.55

11.00  
18.55  
11.00  
18.55

### **Audit commenced at fedpol relating to the activities of the SIRENE office**

At the start of 2018, Switzerland's application of the Schengen acquis in the sphere of data protection was evaluated. As the national supervisory authority for the N-SIS file, in this evaluation the Commissioner commenced an audit of the activities of fedpol's SIRENE office.

On 7 March 2019, at the EU Commission's suggestion, the EU Council decided to draw up some recommendations for rectifying the failings observed during the evaluation of Switzerland's system. Some recommendations involve the Commissioner, and one of these concerns his supervisory role in the SIS. According to this recommendation, the Commissioner must review the lawfulness of the processing of personal data in the SIS more frequently and, at least every four years, conduct audits of data processing operations in the national section of the SIS (N-SIS).

These inspections should not be confined to checking log files, but should also cover aspects such as the structure and functioning of the N-SIS in relation to data protection and should look at data processing operations by the agency responsible for N-SIS, i.e. fedpol – including the SIRENE office and the N-SIS server.

Therefore, as the national supervisory authority for the N-SIS file and in fulfilment of his supervisory remit in connection with the implementation of Schengen, in June 2019 the Commissioner commenced an audit of the activities of fedpol's SIRENE office. The audit focused on alerts in SIS and the exchange of supplementary information between the SIRENE office and its foreign counterparts.

After issuing a questionnaire on the SIRENE office's general activities, the Commissioner made a site visit to check on how an alert is managed in the SIRENE office's system, and how supplementary information is exchanged.

His audit led the Commissioner to conclude that the SIRENE office processes data relating to alerts and the exchange of supplementary information in compliance with Swiss law governing data protection in the sectors covered by the Convention of 19 June 1990 implementing the Schengen Agreement (CISA) and with European law. Consequently, the Commissioner did not issue a decision or take any specific measures.

#### **His investigation covered**

- the structure and functioning of the N-SIS
- the composition of the SIRENE office and its IT system, SIRENE-IT
- the conferring and management of access rights to the N-SIS
- N-SIS access control for staff of the SIRENE office
- the tasks of the SIRENE office with regard to alerts in N-SIS and the exchange of supplementary information with its foreign counterparts, and the description of its identity fraud-related remit
- retention of alerts and supplementary information
- rights of access, rectification, and erasure
- and employee training and awareness

He was therefore able to implement the recommendation made in the 2018 Schengen evaluation and, in so doing, satisfy the conditions of Article 44 of the SIS II<sup>1</sup> Regulation and 60 of the SIS II<sup>2</sup> Decision.

The Commissioner has opened a second audit at the FDJP's IT Service Centre, focusing more specifically on the technical and security-related aspects of the servers .

<sup>1</sup> Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [SIS II Regulation].

<sup>2</sup> Decision 2007/533/JAI of the Council of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [SIS II Decision].

### Schengen Data Protection Act

**The Schengen Data Protection Act (SDPA) entered into force on 1 March 2019 and, with it, some new provisions affecting the Commissioner's current competences (see 26<sup>th</sup> Annual Report, chapter 1.2).**

The SDPA applies in particular to the processing of personal data by federal bodies for the purpose of preventing and prosecuting criminal offences in connection with the implementation of the Schengen acquis. In light of the new requirements and the cross-cutting effect of this new Act on the activities of the offices involved, the Commissioner got in touch with the data protection consultants at the frontline federal bodies likely to be subject to the SDPA, in particular the Federal Office of Police (fedpol), the Federal Office of Justice, which handles mutual judicial assistance in criminal matters, and the Office of the Attorney General, as well as the State Secretariat for Migration and the Federal Customs Administration. Chiefly, the Commissioner was seeking to clarify the scope of this legislation and the new requirements it introduces. Data processing and the federal bodies subject to the SDPA, as well as the Commissioner's competences, were discussed. The Commissioner remains in regular contact with the federal bodies affected by the implementation of the SDPA in their respective remits.

Article 21 of the SDPA tasks the FDPIC with supervising the application of the federal provisions on data protection. Before planning audits in accordance with Articles 21–25 SDPA, it is important for the FDPIC to understand all the processing activities involved that are subject to the SDPA (files/information systems).

For this reason, he asked the Federal Office of Police (fedpol) and the Federal Customs Administration (FCA) to provide us with a copy of the register of processing activities pursuant to Article 12 SDPA and, if they exist or can be generated, statistics for each processing activity (file/information system) for the last five years (2015 to 2019) concerning, in particular, the number of natural and legal persons registered, their nationalities, and the number of users.

## Second Privacy Shield Review

The second Swiss-US Privacy Shield Review took place in Washington D.C. in September 2019. This followed on from the third review of the EU-US Privacy Shield framework and revealed continued progress, along with some further scope for improvement.

Since the Swiss-US Privacy Shield framework entered into force in 2017, more than 3300 companies have signed up to the Swiss-US Privacy Shield and since the last review (see last Annual Report) the number has risen by almost 1000 certifications. Over 70 percent of members are SMEs, but large corporations such as Facebook Inc. and Google LLC remain Privacy Shield-certified (see also <https://www.privacyshield.gov/list>)

In the reporting year, one case was received by the FDPIC for forwarding to the US Department of Commerce. This involved a false claim, i.e. a company falsely claiming to be Privacy Shield-certified. The case was resolved in cooperation with the US Department of Commerce (see 26<sup>th</sup> Annual Report, chapter 1.2).

Ten or so justified complaints against certified companies were also submitted to private, independent alternative dispute resolution (ADR) bodies. Since the framework entered into force, no cases have been submitted to us concerning access to personal data by US authorities for national security purposes.

The functioning of the framework has been improved since the first annual review of the Swiss-US Privacy Shield and the second review by the EU. Now, for instance, the US Department of Commerce undertakes a more systematic review of the certified companies and conducts monthly random inspections, for instance, to establish whether companies are adhering to certain principles laid down in the framework. Moreover, the Federal Trade Commission, which is responsible for enforcement, now has a bigger official role.

The appointments to the supervisory and arbitration bodies are another improvement on the previous reporting year. A permanent ombudsperson has been appointed for the framework, along with the last two missing members of the Privacy and Civil Liberties Oversight Board. There are, however, a few points that are still in need of improvement: The ombudsperson's precise competences are unclear to the FDPIC and the European Data Protection Board. Clarification has been requested. Furthermore, the divergence regarding the question of what exactly is meant by HR data has yet to be resolved.

There is currently a degree of uncertainty owing to a legal dispute that is pending before the Court of Justice of the European Union (CJEU) concerning the transmission of data between the EU and the USA, which could impact on the EU-US Privacy Shield Framework. Although CJEU rulings are not applicable to Switzerland, because the agreements are formulated along the same lines the FDPIC will have to analyse the potential relevance of the CJEU's considerations to the assessment of the Swiss-US Privacy Shield Framework.

## 1.3 Taxation and finance

### Release of personal data to foreign tax authorities – problematic extension to other states

Considerable progress has been made with implementing the new international standards to combat tax fraud and tax evasion. However, the inadequate level of data protection in some countries is proving problematic. During the year under review, we commented on the data protection issues raised by a number of submissions.

### Automatic exchange of information (AEOI)

The global standard for automatic exchange of financial account information (AEOI) took effect in Switzerland on 1 January 2017. Its purpose is to increase tax transparency and thereby prevent cross-border tax evasion. So far, more than 100 countries have espoused this standard, including Switzerland.

The Swiss AEOI network is to be expanded to 18 additional partner states with which the AEOI is to be implemented from 2020/2021; these include states such as Ghana, Kazakhstan, Lebanon and Nigeria. As with previous extensions of the AEOI to additional states, this reporting year the FDPIC kept reiterating the requirement to safeguard an adequate level of data protection in each partner state. If there is no such safeguard enshrined in law, data protection must be assured by sufficient privacy guarantees (see also Art. 6(2) FADP). However, in our estimation, no sufficient guarantees have been created in connection with the AEOI (see 26<sup>th</sup> Annual Report, chapter 1.3).

In an office consultation on the draft of an amendment to the Federal Act on the AEOI (AEIA), the FDPIC commented on the proposed new regulations covering responsibilities in the event that a partner state does not fulfil the OECD's confidentiality and data security requirements. He successfully proposed a different wording which clarifies that, should confidentiality and data security requirements not be met, the competent Swiss authority must suspend the AEOI vis-a-vis the partner state under its own authority; this action is no longer optional. However, the Federal Assembly did not get around to debating the Federal Council's proposal during the reporting year.

### Exchange of Country-by-Country Reports from Multinational Enterprises (CbCRA)

From 2020, for the first time Switzerland will be sharing country-by-country reports from multinational enterprises with its partner states (see 24<sup>th</sup> Annual Report, chapter 1.9.1). During the reporting year, the FDPIC commented as part of an office consultation on the recently announced additions to the list of partner states involved in activating the exchange of country-by-country reports from multinational enterprises. He pointed out that the states and territories to be added appear on the FDPIC's list of countries that have an inadequate level of data protection (such as Armenia, Bosnia and Herzegovina, and the Cook Islands). Therefore, as in previous office consultations the FDPIC stated that additional guarantees as per Art. 6(2) FADP are needed for such countries in order to safeguard an adequate level of data protection (see 26<sup>th</sup> Annual Report, chapter 1.3).

**The Federal Administrative Court backs the Commissioner's objection in the FTA case: affected third parties have the right to be informed in advance**

The Federal Administrative Court upheld an objection by the FDPIC concerning the right to information in international tax-related administrative assistance. The appeal procedure before the Federal Supreme Court has been provisionally suspended.

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 persons) whose names are to be openly, i.e. in unredacted form, transmitted to the foreign authority (see 25<sup>th</sup> Annual Report, chapter 1.9.2). The FTA rejected this recommendation, prompting the FDPIC to refer the matter first to the Federal Department of Finance (FDF), before forwarding the latter's negative decision to the Federal Administrative Court (see 26<sup>th</sup> Annual Report, chapter 1.3).

In its ruling of 3 September 2019, the Federal Administrative Court concluded that, in international tax-related administrative assistance, the persons not affected by administrative assistance requests (third persons) whose data are to be transmitted in unredacted form must, in principle, be informed in advance.



According to the Federal Administrative Court, in cases involving disproportionate effort in order to provide the information, meaning that provision of official assistance would be rendered impossible or excessively delayed, exceptional arrangements must be made. The FDPIC welcomes the ruling, as it protects the fundamental rights of bank staff and other third persons. As he reasserted at a meeting with the FTA in late 2019, he is willing to assist the FTA in seeking practical solutions for implementing the ruling.

The FTA has lodged an appeal with the Federal Supreme Court. At present, the proceedings have been suspended at the FTA's request, as the ruling could be influenced by the decision in another lawsuit. The Commissioner had no opportunity during the reporting year to read the opposing appeal.

## 1.4 Commerce and economy

### **Incorrect database entries at collection agency**

The FDPIC has opened a case investigation at a leading collection firm due to allegedly incorrect entries.

Inquiries from members of the public, and media reports, alerted the FDPIC to a company that provides creditworthiness and credit information as well as collection services. Allegedly, incorrect entries in databases at the company have resulted in confusion between people with the same or similar names or addresses. Consequently, payment demands have apparently been sent to the wrong individuals, or inaccurate negative creditworthiness information has been saved and shared. Difficulties correcting these incorrect entries have also been reported. To look into these accusations, in February 2020 the Commissioner initiated a case investigation. This was still ongoing at the end of the reporting year.

### **Use of Ricardo data within the Tamedia group (TX Group)**

The FDPIC continued his case investigation into the use of data collected by the ricardo.ch platform, in particular within the Tamedia group (TX Group).

In July 2017, we began a formal procedure to investigate the transparency and compliance of the processing of data relating to users of the ricardo.ch platform within the Tamedia group, and the options for objecting, in particular, to the use of data for targeted advertising. (see 25<sup>th</sup> Annual Report, chapter 1.8.8).

Since the procedure began, the situation has changed appreciably: among other things, the privacy statement was revised in May 2018, when the European General Data Protection Regulation (GDPR) came into effect (see 26<sup>th</sup> Annual Report, chapter 1.4.), then again in March 2019 and February 2020.

Tamedia AG (which has since changed its name to TX Group AG) processes, analyses and aggregates personal data collected on the ricardo.ch online shopping platform, in particular for marketing purposes (targeted advertising); therefore, we formally extended the procedure to include Tamedia AG. We re-submitted our findings for review, and made a few changes. Our legal assessment will be based on the observed facts.

### **Incorrect addresses at Serafe AG – Data accuracy measures needed**

In the reporting year, Serafe AG sent out thousands of incorrect invoices. The company recognised the issue and has taken initial action. The FDPIC is investigating the need for further privacy recommendations.

Serafe AG has been the Swiss billing agency for the radio and television licence fee since early 2019. Following a public procurement process, the Federal Department of Environment, Transport, Energy and Communications (DETEC) awarded it the mandate until the end of 2025.

Serafe AG sent out thousands of incorrect invoices during the reporting year, attracting media coverage and prompting data subjects to contact the FDPIC. Some invoices were sent to out-of-date addresses or to the wrong addressees, or were sent multiple times to the same recipients.

Allegedly, some of the data needed to bill the household fee were inaccurately supplied by the cantonal and



communal registers of residents. However, we are told that the issue has been identified and measures have been taken to guarantee the accuracy of data in future.

The Commissioner has asked Serafe AG for comment. Depending on the answers he receives, he may decide to undertake an investigation into privacy aspects and, if necessary, suggest further measures to the people responsible in order to guarantee the compliant processing of data.

### **Transactional data analysis for planning purposes**

A brand approached the FDPIC for an opinion on the use of its customers' transaction data for purposes not linked to individuals. Within our consultancy mandate, we reviewed and evaluated the project from a technical and legal perspective.

The brand, which is involved in retail and has a number of stores in Switzerland, outlined to us its plans to use its customers' transaction data for purposes not linked to individuals, as part of its business planning.

According to the concept presented to us, the data collected by the brand at the time of the transaction on one side, and the data recorded by the payment service provider on the other side, would be used. The combination of the available data would enable the brand to monitor transactions effected using a particular payment card and to establish a spending profile over time (transverse profile), which the company is unable to do with only the data at its disposal. However, the brand stated that said analysis would be performed exclusively for purposes not linked to individuals (in particular, it would not be used for targeted advertising).



As the brand does not capture data on the payment card, the payment service provider would have to first supply these data. To this end, the concept proposed replacing the payment card number with a unique identifier (“token”), generated at the end of a hash process (pseudonymisation).

In our consultancy capacity, after completing a technical and legal assessment of the documents supplied we concluded that both the processing of data by the payment service provider and the processing of data by the brand were subject to the FADP, as in all instances the data being processed are without doubt personal data.

Assigning a unique identifier (using the hash function) makes the data harder to identify and minimises the invasion of privacy, in accordance with the principles of proportionality and

security. The other general privacy principles, such as the purpose and transparency principles, also apply.

The sharing of the data by the payment service provider constitutes a change of purpose compared with the initial processing of the data (which is to provide the payment service); such a change of purpose must be justified – in this instance by the voluntary and informed consent of the customer concerned. As regards technical measures, we stressed the need for security purposes to use a hash function with a salt or secret key.

We took the view that the brand could claim an overriding private interest pursuant to Article 13(2)(e) FADP, provided it respects the stated terms: the personal data must be processed for purposes not linked to individuals, but for research, planning or statistical purposes; moreover, the results must be published in a form that does not allow identification of the persons concerned. On this basis, therefore, the knowledge obtained from analysing profiles cannot be used in this instance for targeted advertising and the brand cannot combine this knowledge with other personal data at its disposal (loyalty card, e-shop or other). To do otherwise would entail profiling, and such use would require the explicit consent of the data subjects.

The brand acknowledged receipt of our assessment and will inform us if it implements the plans.

### **Sporting goods retailer Decathlon provided inadequate information about data procurement**

*As part of a case investigation, the Commissioner demanded that Decathlon provide better information to its customers when gathering data. The sporting goods retailer has revised its privacy statement.*

In 2018, we opened a case investigation at sporting goods retailer Decathlon, after learning from various sources that it was making sales of goods in its Swiss stores contingent on the disclosure of certain customer data. After the investigation began, Decathlon told the FDPIC that customers had to provide their e-mail address or telephone number in order to purchase goods in-store. In future, it said, the company would not make the sale of goods contingent upon the provision of this data and would only collect the data on a voluntary basis. This prompted the FDPIC to consider whether the voluntary nature of this was indeed apparent to customers, and whether they were

being properly informed when the data was obtained. As the information from Decathlon was inconsistent, and the wording lacked



clarity, the FDPIC made proposals to the sporting goods retailer for improving the information. (see 26<sup>th</sup> Annual Report, chapter 1.4). In the reporting year, Decathlon took account of all of the FDPIC’s suggestions and completed the revision of its privacy statement.

## Authentication using voice recognition at PostFinance AG

In the reporting year, PostFinance AG contacted the FDPIC and presented to him its project for voice recognition at its contact centre. The Commissioner pointed out to the company that, since they are biometric data about individuals, voiceprints carry a heightened risk and, as such, require special protection.

During the reporting year, PostFinance AG presented to the FDPIC a project for the use of voice recognition to identify people who telephone the contact centre. The caller's identity is verified by comparing the voice against a recorded voiceprint. PostFinance AG stressed that the voiceprints collected would be used solely and exclusively to authenticate customers on the phone. It says it has no plans at present to use these data for further analyses.

In contrast to the EU's General Data Protection Regulation (GDPR), the Swiss FADP does not list biometric data under sensitive personal data – despite the special risks inherent in their processing. Biometric characteristics are inseparably associated with a particular individual and, unlike passwords, cannot be changed following a fault or their misuse. In light of the technical progress made by voice and facial recognition programmes (see article on Clearview in chapter 1.1) and the resulting, heightened risks to data subjects' privacy, the processing of biometric data using such technologies must guarantee a higher level of data protection. For cases in which, according to the FADP, consent must be obtained, the FDPIC therefore believes such consent must be explic-

itly obtained before data may be collected. Furthermore, the data holder concerned must provide transparent and full information about the data processing in advance.

As part of his consultancy role, the FDPIC demanded that PostFinance AG introduce such a procedure, which – initially – the company duly did. However, PostFinance AG subsequently altered the process and now merely offers Swiss customers an opt-out. This means that, in principle, voice recognition is used for callers unless they explicitly object to it.

We asked PostFinance AG for a written comment, particularly as we have noted that, in the case of foreign customers, voice recognition is not used until they have given their explicit consent, i.e. an opt-in arrangement. In its comment the company confirmed that, having obtained a third opinion during a fresh review of legal compliance, it altered the process at the end of 2018. The procedure now involves the use of an automated prompt to inform Swiss customers about the recording of their voiceprint. If customers do not agree to their voiceprint being created, they must proactively inform the customer advisor that they do not consent, or subsequently disable the function in their e-finance portal. PostFinance AG stated that, for foreign customers, there is a chance that more stringent data protection rules apply, such as the GDPR; thus prior, explicit consent would continue to be sought from them.

The FDPIC took note of PostFinance AG's comments and issued a public statement pointing out the urgent need to raise the level of data protection for the Swiss public. Until the complete revision of the FADP enters into force (see also the focus on the revision of the FADP in this report), Swiss customers evidently cannot be certain that all companies here treat them on the same footing as foreign customers.

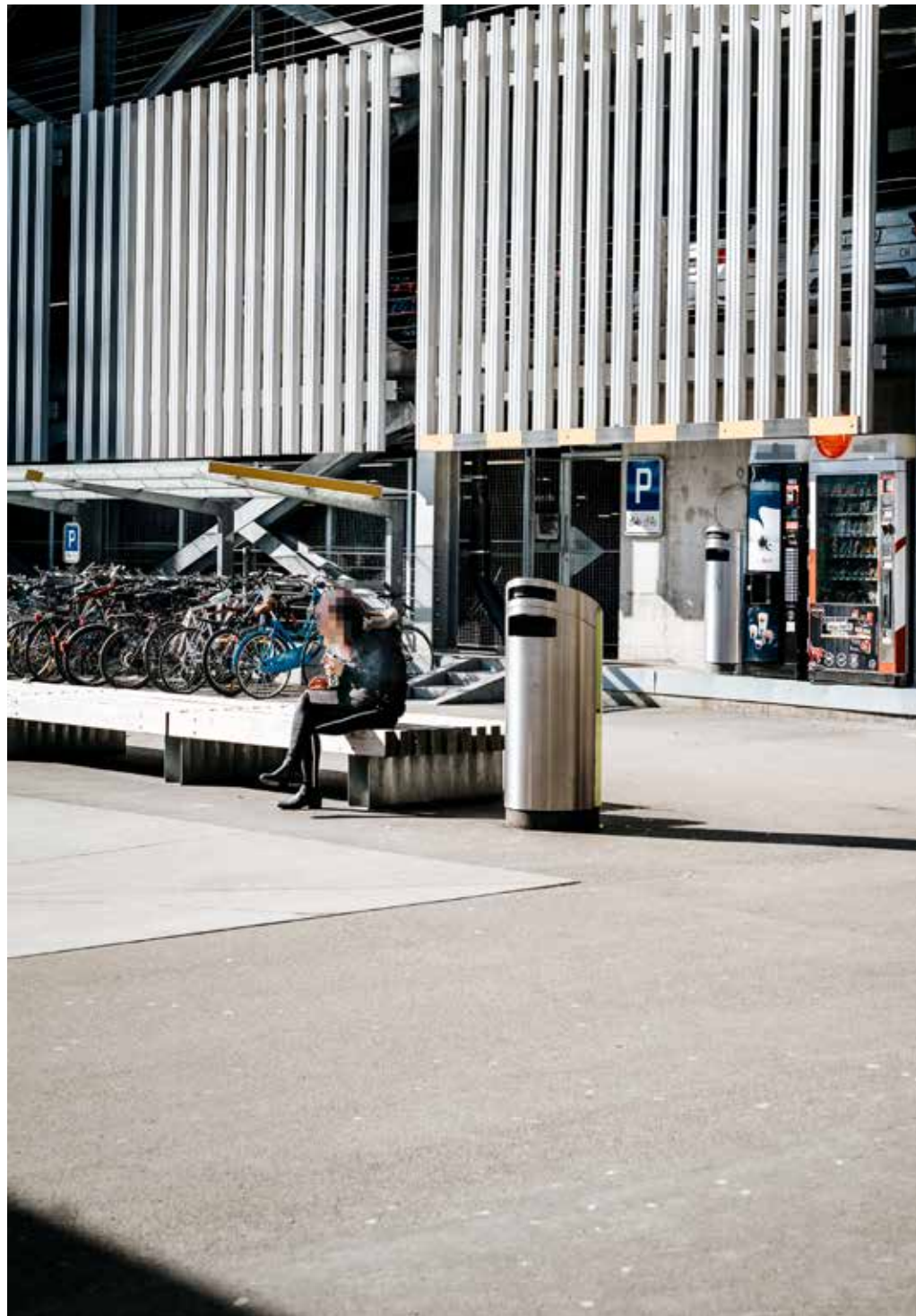
## Video surveillance using intelligent cameras at Migros

During the reporting year, Migros trialled a new camera system for surveillance in its stores. The FDPIC is reviewing privacy compliance.

The FDPIC was alerted by media reports to the fact that Migros is using novel surveillance cameras. When contacted by the FDPIC, Migros stated that it was testing a new system in a pilot project in some of its branches. The software used enables customers to be analysed based on certain appearance criteria in the event of an incident, and the relevant video sequences can then be reviewed. However, according to Migros the new cameras are not used for facial recognition.

This raises a number of questions for the FDPIC with regard to the privacy-compliant design of such systems. Specifically, transparency towards data subjects and safeguarding high security standards in data processing are

key concerns. Following his preliminary investigations, the FDPIC opened a case investigation to review the system in depth and, if necessary, make privacy recommendations. This investigation was still ongoing at the end of the reporting year.



## 1.5 Health

### Dialogue stepped up prior to launch of electronic patient records

From 15 April 2020, Swiss nationals are to have access nationwide to electronic patient records (EPRs). In light of this imminent launch, EPRs remained a priority for the FDPIC during the reporting year – more specifically the providers, or reference (or “core”) communities.

EPRs give individuals digital access to their personal health data, such as illnesses and medicines to be taken, and allow them to decide who can view those data. The introduction of electronic patient records, which is scheduled for 15 April 2020, was responsible for a continued increase in the number of inquiries to the FDPIC from members of the public. We also redoubled our coordination efforts with the cantonal data protection commissioners and helped stage a number of specialist events.

Due to the importance and topicality of the issue, the FDPIC also obtained first-hand information from one of Switzerland’s biggest reference communities about the status of work, implementation, and the difficulties involved in introducing EPRs. By law, these bodies have exclusive authority to provide EPRs and are subject to supervision by the FDPIC, whilst the predominantly cantonal institutions such as hospitals are supervised by the cantonal data protection commissioners. In this way, the FDPIC gained an overview of the set-up work, and of the complex technical processes and instruments needed to operate EPRs. It became apparent that it is not just the creation of the reference communities that presents a technical challenge; the certification process itself is also very complicated for the reference communities and for the issuers of the means of identification needed for the electronic identity in EPRs involved.

According to information from the agencies involved, the roll-out will be delayed until the summer of 2020. The FDPIC will continue monitoring developments and will give consideration to the necessary checks as soon as the reference communities are operational.

### “Helsana+” bonus programme – Implementation of the Federal Administrative Court ruling

In 2019, the Federal Administrative Court judged certain types of data processing undertaken by the insurer as part of the “Helsana+” bonus programme to be unlawful. The FDPIC was in touch with Helsana several times during the reporting year, to make sure that the ruling was being fully implemented and that future changes to the terms of use satisfy the data protection requirements.

In its ruling of 19 March 2019, the Federal Administrative Court found the obtaining of data by the health insurer in the original manner to be unlawful, as no legal consent was obtained. (see 26<sup>th</sup> Annual Report, chapter 1.5). In its considerations, the court identified certain shortcomings in the terms of use and privacy provisions of “Helsana+” which, the FDPIC believes, exist regardless of the question of legal consent. After the ruling took effect, the FDPIC therefore demanded that Helsana eliminate the identified shortcomings in the Helsana+ terms of use and privacy provisions, in order for the provisions to satisfy the requirements of transparency and clarity.

Since then, the insurer has comprehensively revised the terms of use for the bonus programme. With a particular view to the new arrangements, the FDPIC is continuing to liaise with the insurer to ensure privacy-compliant data processing.

**“Swiss National Cohort”:  
additional precautions  
necessary**

The “Swiss National Cohort Study (SNC)” research project has mushroomed and is now giving rise to matching. Therefore, the data processed are no longer anonymous and tighter privacy arrangements must be established.

In partnership with the Federal Statistical Office (FSO), the Epidemiology, Biostatistics and Prevention Institute (EBPI) of the University of Zurich and the Institute for Social and Preventive Medicine (ISPM) of the University of Bern joined forces in 2006 to create the first cohort representing the whole Swiss population over the long term and hence a broadly-based research platform. In response to a request from the ISPM, we issued our opinion on privacy compliance by the SNC, with due consideration for the competences of the cantonal data protection authorities involved.

We found that adequate technical and organisational measures were in place to safeguard the security and accuracy of the data. However, unlike the previous phases of the project, we observed that a lot of rich personal data, including health data, were being matched, making anonymisation impossible. Therefore, we advised the sponsors of the project to take additional precautions to safeguard the confidentiality of the subjects’ data.

**IQOS: Investigation into the next generation IQOS e-cigarette by Philip Morris**

**IQOS electronic cigarettes by Philip Morris produce neither a light nor ash, but a huge amount of data. The Commissioner investigated the privacy compliance of data management.**

The e-cigarette market is growing, and Parliament is currently drafting a law on tobacco products and electronic cigarettes. Over the last few years, Philip Morris has developed a new product: made up of tobacco sticks called “heets” and a device that heats them without burning them, “IQOS” also has a Bluetooth connection which enables data to be exported from the system. IQOS is thus not just an electronic cigarette: it is a connected object. As several newspaper articles raised concerns about IQOS and data protection issues, on 11 July 2019 our authority opened a case investigation to determine whether data processing in connection with IQOS is likely to violate the privacy of consumers in Switzerland.

Our investigation focused on compliance with legal requirements regarding information, consent and cross-border communication of data, both within and outside the multinational corporation. We found that the technical and organisational measures taken by Philip Morris were adequate to safeguard the privacy of users in Switzerland.



## 1.6 Employment

### Time recording and tracking with apps in the work environment

With apps to record working time, or register routes travelled during work, smartphones are playing an ever-greater role at the workplace. If these apps are to be privacy-compliant, it is particularly important for data processing to be kept to the necessary minimum, and for employees to be adequately informed.

There was a further rise in inquiries from members of the public during the reporting year concerning mobile applications in the work environment. What with time recording, GPS tracking and access to business e-mails, there are scarcely any areas of working life that cannot be dealt with on a mobile phone. As well as making our everyday work simpler, the mobile office in our pocket does present a few privacy challenges, particularly as many of these technical functions can be used in addition to employee monitoring.

Privacy-compliant use of mobile apps in the work environment means that the employer only processes those personal data of its employees that are necessary in order to fulfil the employment relationship. Furthermore, the processing principles of the FADP

must always be observed, including proportionality and transparency. Where transparency is concerned, it is often the case that

employees are not properly informed as to how, or why, monitoring is undertaken.

The technical and organisational measures designed to prevent misuse of data and access by unauthorised persons, including within the company, present a further challenge. Lastly, what happens to data recorded by GPS tracking after the working day ends, or during breaks, is often unclear; in principle, any such processing of data is a breach of employee privacy. The frequency of requests by data subjects for our advice on this matter is therefore unsurprising.

The issue surrounding the ‘logging’ of working life on a mobile phone is compounded if that same smartphone is used for private and professional purposes. In particular, this begs the question: what is the correct procedure following termination of employment?

The FDPIC will continue carefully monitoring developments surrounding mobile applications in everyday working life, and has also initiated a case investigation (see box).

#### Case investigation into time recording

The FDPIC has begun a case investigation into a large building cleaning and maintenance company. The company has a very sizeable workforce, and recently digitalised much of its time recording. The registration of working hours, which is now done online, raises various privacy issues, particularly with regard to data security, access rules, and data flows within the company as well as to any third parties. When the procedure is complete, the FDPIC will publish the findings of the case investigation.

### **Use of artificial intelligence in the application process**

Artificial intelligence (AI) is being used increasingly often in application processes, giving rise to invasions of privacy that are often more serious than in conventional recruitment processes.

Several media reports and inquiries during the reporting year suggest that there is also increasing reliance on artificial intelligence (AI) in recruitment processes in Switzerland. One example is the video recordings of interviews, for subsequent analysis by software.

The privacy framework when using these new instruments is, on the face of it, the same as in conventional application processes: the employer may only collect and process the data necessary to ascertain a person's suitability for the job concerned, and it must always abide by the privacy principles.

However, given the plethora of analysis options allowed by AI-based processes, invasions of privacy tend to be a more serious concern than in conventional interviews. Therefore, particular attention must be paid to the principles of identifiability and proportionality.

Investigations at the Federal Office of Personnel (FOP) revealed that the Confederation does not currently use artificial intelligence in its application process. Should it plan to do so in future, the FDPIC will intervene at an early stage, and demand the moderate and privacy-compliant use of the technologies involved.



## 1.7 Insurance

### **New legal provisions take effect on observations in the social insurance system**

The new legal bases for the surveillance of insured persons have been incorporated in the Federal Act on General Aspects of Social Security Law (GSSLA) and entered into force with the related ordinance on 1 October 2019. During the reporting year, we advised litigants who contacted us about surveillance.

The “observation article”, as it is known, introduced changes to surveillance in the social insurance system during the reporting year. Articles 43a and 43b of the Federal Act on General Aspects of Social Security Law (GSSLA) and the related implementing provisions of the ordinance in articles 7a–9b GSSLO established the relevant legal bases with effect from 1 October 2019.

These regulate the requirements and permissible means of covert observation of insured persons who are suspected of an insurance abuse. A legal framework in this area was necessitated by the ruling of the European Court of Human Rights (ECtHR) in Strasbourg in the case of “Vukota-Bojic versus Switzerland” of 18 October 2016 (complaint no 61838/10), in which the Court found that Switzerland lacked a sufficient legal basis for the use of private detectives in the area of social insurance. The ECtHR took the view that the surveillance measures undertaken by insurance companies were a violation of privacy, which is protected by Article 8 of the European Convention on Human Rights (ECHR).

As the Commissioner believes that such observations materially affect the protection of privacy, he got involved in the legislative process at an early stage. Among other things, he demanded that observation may only be ordered by a person in a senior management role in the department dealing with the case or in the operational area of the insurer concerned. He also called for the duration of surveillance to be limited by law. Both aspects were incorporated in Article 43a GSSLA.

Prior to this change in the law, private detectives could only be used for observations in the sphere of invalidity insurance and accident insurance.

Now, observations are permitted in the other branches of social insurance: unemployment insurance, compulsory health insurance, military insurance, supplementary benefits, income compensation allowances relating to national service and maternity, and old-age and survivors’ insurance. As quite a few of these insurances are administered by cantonal offices, meaning they can order observations, these surveillance activities are supervised by the respective cantonal data protection commissioners. The FDPIC, meanwhile, is responsible for supervising and advising on data protection matters involved in accident insurance, health insurance and military insurance and, therefore, observations ordered in connection with these types of social insurance.

## **Draft legislation on the systematic use of the OASI number**

On 30 September 2019 the Federal Council presented a dispatch to Parliament on an amendment to the OASI Act. Under the draft, the federal, cantonal and communal authorities will be authorised to systematically use the OASI number as a unique identifier outside the sphere of social insurance. This proposal also draws to a conclusion a development that has been underway for many years, over the course of which the federal legislators have extended the use of the OASI number way beyond the social insurance system in numerous special laws. Consultations on the modernisation of commercial register and land register law also threw up discussions about the wider use of the OASI number, in which the FDPIC was invited to participate by the Legal Affairs Committees of both Councils. After we persuaded the Federal Office of Justice to commission a study by ETH Zurich assessing the privacy risks, which served as input in the consultations on the modernisation of the land register, it became clear that the federal, cantonal, and communal registers of persons are vulnerable to unauthorised and improper access. However, the expert also confirmed that, on their own, sectoral identifiers like those provided for in federal legislation for tasks such as the management of electronic patient records do not significantly reduce these privacy risks. After taking note of the findings, in 2017 the Legal Affairs Committee of the National Council instructed the Federal Council in a postulate to present a proposal for reducing the risks identified by the

study, with due consideration of the FDPIC's opinion. (see 26<sup>th</sup> Annual Report, chapter 1.1.2).

The Federal Council fulfilled this instruction in the aforementioned dispatch, and our authority was also consulted at length by the Federal Social Insurance Office when preparing the dispatch and draft legislation. Our suggestions and comments were taken on board. In light of the serious privacy risks, we welcome the fact that the draft law explicitly obliges entities operating databases in which the OASI number is routinely used to carry out periodic risk analyses with a particular focus on the danger of unauthorised data matching. Based on this risk analysis, state-of-the-art security and data protection measures must be implemented that are commensurate with the risk involved. We also welcome the requirement for the entities named in the bill which routinely use the OASI number to keep a register of relevant databases which, in particular, can be used as a basis for the required risk analyses. We also welcome the Federal Council's assurance that the consistent use of the OASI number cannot be allowed to override the constitutional boundaries of the administration's responsibilities and the FDPIC will hold the federal administration to account in this respect. The Federal Council also stresses that the standardised use of the OASI number must not lead to the social security number being used as a general means of identification, as in the USA or Scandinavia, where there have been repeated, mass identity thefts. He wants to counter this by limiting use of the number by the private sector and making it a legal requirement for state officials to be trained in using the

OASI number solely for specific remits. In future, the electronic identity will be available for identification purposes in communications between government authorities. As is still permitted under the new version of the OASIA, this will be based on an E-ID registration number that is separate from the OASI number. This too is welcomed by the FDPIC.

The technical requirements of the proposal are also significant; among other things, datasets containing the OASI number must, in future, be encrypted when transmitted over the public network.

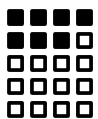
Having been asked to speak before the Political Institutions Committee of the Council of States at its meeting on 18 February 2020, we used the opportunity to reiterate the importance of concrete safeguards and measures to minimise risks and, in this context, the need for the Confederation, the cantons and the communes to gradually review the design of their database architecture.

## 1.8 Traffic and transport

### New public transport app SmartWay creates personality profiles

New public transport apps are constantly being developed. In this context, the FDPIC has specifically advised SBB (Swiss Federal Railways), which has launched mobility apps including EasyRide for electronic ticketing and the electronic travel assistant SmartWay during the reporting year.

As the number of travel-related apps on the market continues to grow, in recent years the FDPIC has advised a number of transport companies on various aspects, in particular electronic ticketing. (see 24<sup>th</sup> Annual Report). The FDPIC's dialogue with transport companies continued over the last reporting year, in particular with SBB's data protection officers, on subjects including the use of Fairtiq technology for electronic ticketing. Among other things, the FDPIC ensured that the terms of use for Fairtiq-based EasyRide are worded in a more customer-friendly way, with due regard for proportionality. Moreover, he also obtained an assurance that the restrictions on the sharing of data and the processing of data by third parties will be observed in practice.



Furthermore, at a meeting SBB presented to the FDPIC the extremely data-intensive SmartWay app, which is still in the test phase. This app makes personalised travel recommendations to users, with suitable connections. The app records data continuously, 24 hours a day, regardless of whether the app is being used or not. Users cannot reject this function and, unless they actively delete the data or do not use the app for a period of several months, the data are only erased after four years.

After just a few days, personality profiles are created, and it is virtually impossible to anonymise mobility profiles. Consequently, very high data protection requirements must be set, particularly with regard to proportionality and information. The FDPIC insisted that users must be fully and clearly informed about all the ways in which their personal data are processed before they register, to enable them to give voluntary consent. It must be clear to them who processes which data, and for what purpose. Moreover, consents must be explicitly obtained ("opt-in"), and must be specific rather than general. The manner in which the right to information can be exercised, including when data are processed by third parties, must be explained, and users must be told whether the profiles are also deleted by any third parties, if they are deleted in the app. If they are not, users must be informed how they can delete all their data.

If data are processed abroad, for example in a cloud, users must be adequately informed and the country for information and deletion requests must be named.

On a general note, third parties that process the personal data must themselves abide by the data protection



principles and data security.

The FDPIC pointed out that data processors are responsible for safeguarding data protection from the outset, and for performing regular risk impact assessments throughout the project development phase

## **Audit of a pilot project by SBB and Axon Vibe**

During an extended interruption to rail services between Lausanne and Puidoux-Chexbres, SBB launched a pilot project to compensate customers. The FDPIC carried out a case investigation into the proper processing of data.

In the summer of 2018, SBB had to close the railway line between Lausanne and Puidoux-Chexbres for several months due to engineering work. SBB launched a pilot project to fairly compensate railway customers who were hit by multiple, severe delays. The project involved automatically recording journeys made by the SBB customers involved in the compensation project using the geolocation and “Movement and fitness” functions on a smartphone. Among other things, customers’ movement data were processed. As this raises some privacy-related issues, the FDPIC decided to undertake a case investigation into the processing of personal data.

The aim of our audit was to check whether SBB was, as it had assured us, processing personal data in accordance with the law. Of particular interest was the exclusive use of the personal data for this pilot project, and the deletion of the data. We also focused on the transmission of data by SBB to Axon Vibe and the further processing of those data by that third company.

During the case investigation it became clear that various privacy-related aspects had implications beyond the pilot project that was the focus on our case investigation. For example, the data relevant to the pilot project were recorded via a more extensive system (Travel Cockpit), which already contained customer data. There was no evidence of a clear demarcation between these data and those collected for the pilot project.

Among other things, it was not clear whether SBB or Axon Vibe was the responsible data processor.

A detailed analysis would have required a new, more extensive case investigation. The pilot project covered a very small area and timeframe, so relatively few customers were affected and SBB has now launched more data-intensive apps on which the FDPIC is focussing. Therefore, the FDPIC confined his investigation to the proper, irretrievable deletion of all the personal data collected as part of the pilot project.

Our correspondence with SBB and Axon Vibe was still ongoing at the end of the reporting period.

## **Protection of privacy in the Mobility Pricing project**

As Switzerland’s population is expected to grow to 10 million, the Federal Roads Office (FEDRO) is planning to influence the public’s mobility behaviour through travel costs. This “mobility pricing” will depend on the time of day and the distance covered, as well as the means of transport used. The project is in its infancy. The FDPIC is demanding that privacy requirements be factored in at an early stage.

The Federal Roads Office is assuming that Switzerland’s expected population of ten million in around twenty years would overstretch the current transport system. According to FEDRO, neither the traditional infrastructure can be expanded to the necessary extent, nor would visionary systems such as underground structures be available on time. Therefore, to avoid traffic peaks, FEDRO intends to focus on solutions which influence the public’s mobility behaviour. Mobility pricing, as it is called, will charge transport users in accordance with the distances they cover in Switzerland, depending on time of day and means of transport used.

Implementing this system is reliant on recording transport users’ mobility patterns and, therefore, processing sometimes sensitive personal data and movement profiles. (see above).

At present, the Commissioner is assuming that it is possible to design a privacy-compliant Mobility Pricing system. Over the course of the reporting year, the FDPIC attended a number of meetings with FEDRO and issued written comments to keep the focus on implementing privacy early on in the project. Our particular priority is that all official bodies and private companies involved in the project must have an internal data protection consultant, with adequate resources at his/her disposal. The data protection consultants must be involved in the project early on, to ensure that the



necessary risk impact assessments are undertaken and privacy-friendly technologies are developed. The

resources needed for this must be budgeted from the outset. Furthermore, privacy-related documentation must be prepared.

### **Cyclomania app by Pro Velo Schweiz**

**A new app to promote the use of bicycles will track registered users for one month. The FDPIC advised Pro Velo Schweiz on data protection aspects.**

The national umbrella organisation of local and regional associations representing the interests of cyclists in Switzerland (Pro Velo Schweiz) is developing the new Cyclomania app, with the support of the Federal Office of Energy. The app is intended to help promote the bicycle as a means of transport. For one month, the app creates a mobility profile of registered users. The data collected are used for personal statistics of Cyclomania users and to hold prize draws. Additionally, the data will be made available to the communes in anonymous or aggregate form, to enable them to improve their infrastructure in line with the general public's behaviour. With users' consent, the data will, if appropriate, be retained for research purposes beyond the timeframe of the campaign.

The FDPIC advised Pro Velo Schweiz on the privacy-related aspects of the project. Among other things, it is important that users are transparently and adequately informed about all the ways in which their personal data are processed, and that the proportionality principle is observed. For example, the data must be deleted once they are no longer required for the purposes indicated.

Furthermore, it must be as straightforward as possible for the user to switch off the app, or use it for a specific purpose, by selecting and changing certain privacy-friendly settings and defaults. It would make sense to keep the information and explicit consent brief and easily comprehensible, with clickable links to further information. The impossibility of anonymising mobility profiles must also be borne in mind (see chapter 1.1).

## 1.9 International

### **International Conference of Data Protection and Privacy Commissioners ICDPPC in Tirana**

We attended the 41<sup>st</sup> International Conference of Data Protection and Privacy Commissioners, the topic of which was “Convergence and connectivity: raising global data protection standards in the digital age”. The conference stated its intention of strengthening its position as a global forum.

The 41<sup>st</sup> International Conference of Data Protection and Privacy Commissioners was held in Tirana, from 21 to 24 October 2019, under the aegis of the Albanian Commission for Personal Data Protection. The conference began with a closed session, during which members agreed on a framework which will continue strengthening the group’s position as an international forum. This session heralded the beginning of a new phase of collaboration among data protection authorities the world over. The new name chosen for the International Conference, “Global Privacy Assembly (GPA)”, is a milestone in a process of reforming the conference’s internal organisation, functioning and coordination going forward. The conference’s three strategic priorities are, firstly, to promote privacy protection around the world in the digital era; secondly, to maximise the conference’s voice and influence, in particular by strengthening the conference’s role in digital policy and relationships with other international bodies and networks; and, thirdly, to strengthen capacities in order to help members share their expertise throughout the year.

Six documents were adopted during the closed session on 21 and 22 October 2019:

- Resolution on the Conference’s strategic direction (2019–2021);
- Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights;
- Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement;
- Resolution on social media and violent extremist content online (the FDPIC opposed this proposal and, along with representatives of other data protection authorities, abstained from the final vote);
- Resolution to support and facilitate regulatory cooperation between data protection authorities and consumer protection and competition authorities to achieve clear and consistently high standards of data protection in the digital economy;
- Resolution to address the role of human error in personal data breaches.

Albanian Prime Minister Edi Rama gave a speech during the Conference’s open session. The main feature of this open session was interaction and cooperation between the representatives of data protection authorities (DPA), academia, industry, civil society and the media. Discussions covered opinions on common data protection and privacy standards; global challenges with regard to protecting privacy in commercial data-based models; data protection and competition as a converging digital regulatory framework; as a global body, playing an enabling role in achieving high data protection standards; and, lastly, discussions about the future challenges facing data protection authorities and data protection officers.

More than 700 people attended the Conference. The next conference is scheduled to be held in Mexico in 2021.

## **Conference of European Data Protection Authorities in Tbilisi**

We attended the Conference of European Data Protection Authorities, which focused on the challenges of implementing the GDPR and the major innovations introduced by Convention 108+. This Convention is still the only legally binding international instrument in the sphere of data protection.

The Conference of European Data Protection Authorities was held in Tbilisi (Georgia) on 8, 9 and 10 May 2019, at the invitation of the Georgian Data Protection Commissioner. This 29<sup>th</sup> Conference was an opportunity to review the first year in force of the EU GDPR, providing a venue for the data protection authorities to join in debates on the challenges involved in implementing and applying the GDPR. In this context, various actions taken by the data protection authorities were presented, among them a software package by the French data protection authority CNIL which can be used for a Data Protection Impact Assessment and is available in 16 languages. A panel discussion, which included a representative of the FDPIC, discussed the territorial scope of the GDPR and the cooperation mechanisms.

Participants also discussed Convention 108+ of the Council of Europe which, in particular, will facilitate cooperation among the parties, the protection of children's data, the protection of international data and organisations, and the future of the conference. The main innovations introduced in Convention 108+ were presented by experts on the panel, all of whom reiterated that the entry into force of this Council of Europe document was vitally important to everyone, since it remains the only legally binding international instrument in the data protection sphere.

## The Francophone Association of Data Protection Authorities

A representative of the FDPIC attended the annual Conference of the Francophone Association of Data Protection Authorities (AFAPDP) in Dakar, the theme of which was “the digital citizen”. Striking a balance between protecting individuals’ privacy and the interests of all stakeholders is the biggest challenge facing data protection authorities.

The Francophone Association of Data Protection Authorities (AFAPDP) held its conference in Dakar, on 16 and 17 September, at the invitation of the Senegalese Commission for Personal Data Protection and with the support of the “Organisation internationale de la Francophonie”. Fourteen delegations were represented at the Conference. The presidents, commissioners and representatives of the French-speaking personal data protection authorities also welcomed the Office of the Information Commissioner (OIC) of Jersey, bringing the membership tally to 21. The ICDPPC and the Telecommunications Regulatory Board (ART) of Cameroon were in attendance as observers. The members elected a new executive committee. Finally, an action plan until 2025 was adopted. This plan is designed to help achieve the association’s three main objectives: promote the right to protection of personal data and privacy in the French-speaking areas, support and strengthen the capacities of AFAPDP members, and disseminate expertise and the French-speaking vision beyond the borders of their regions.

The theme of the annual conference was “the digital citizen”. In the digital space, the legal subject is viewed as a consumer, a study subject, or an anonymous troll, as if the digital space were separate from real life and individuals must inhabit one of two separate compartments. Striking a balance between protecting individuals’ rights and safeguarding the interests of data controllers, without losing sight of the progress and infinite possibilities contained within the digital realm, is the daily challenge facing data protection authorities. Personal data are indissociable from the individual person. It is important that our authorities constantly remind themselves of the very essence of their role, which is to protect individuals’ privacy.

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

The Supervision Coordination Groups met in Brussels during the year under review. They discussed matters including the exponential increase in information requests concerning the SIS information system, and adopted two reports.

As a national supervisory authority, the FDPIC again attended the meetings of the three Supervision Coordination Groups on the EU’s SIS II, VIS (chaired by the FDPIC) and Eurodac information systems. The meetings were held on 19/20 June 2019 and 26/27 November 2019, in Brussels. The European Data Protection Supervisor (EDPS) and the national data protection authorities of the member states were represented.

The SIS Supervision Coordination Group focused in particular on the huge increase in information requests concerning the SIS information system. Many member states experienced an increase, but no country more so than Switzerland. The Supervision Coordination Group will continue focusing on this issue. The Eurodac Supervision Coordination Group adopted the report on the rights of data subjects and the VIS Supervision Coordination Group adopted the report on data protection training for people with access rights to the VIS.



All three groups also discussed the planned change to their structure. In future, the three supervision coordination groups will form a 'Coordinated Supervision Committee' within the European Data Protection Board (EDPB), which will also manage their secretarial activities. Although Switzerland is not a full member of the EDPB, it has a status as observer in areas relevant to Schengen and Dublin.

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

[The working party on 'Data Governance and Privacy in the Digital Economy', which was recently founded by the Organisation for Economic Cooperation and Development \(OECD\), held its first meeting in November 2019, in Paris.](#)

As well as establishing the newly-created working party, a day-long expert meeting was held on the subject of 'meeting new challenges in the enforcement of data protection'. On the second day, a number of topics and working papers were discussed and forwarded for further processing to the secretariat and, from there, for member consultation.

The first roundtable looked at the impact of artificial intelligence on the protection of personal data and on the implementation of data protection guidelines. Among the questions addressed were: What challenges does artificial intelligence present to data protection authorities when enforcing the fundamental data protection principles of the data protection guidelines and during audits? To what extent do the current guidelines of AI policies take account of privacy and data protection? How can the exercise of individuals' rights be safeguarded?

The second roundtable explored the increasing cross-border flow of personal data and the growing importance of international cooperation in upholding privacy and data protection. Various opportunities for cooperation were identified and questions including the following were discussed: How can international cooperation help establish trust in the cross-border flow of personal data? What are the obstacles to international cooperation, and how can they be overcome? What are the lessons from collaborations?

At the third roundtable, conclusions were drawn from the day's discussions and consideration was given to how the OECD can best respond to the challenges.

At the closed meeting, initial drafts of interim reports, surveys and working papers were discussed, covering the following subjects: improved access to, and shared use of data, data portability, data ethics, the practicalities of deploying artificial intelligence, and how to improve the comparability of reports of privacy breaches. Furthermore, the working party looked at the recommendation made in 2012 on the protection of children online, which is currently under revision. Finally, the secretariat presented an initial interim report on the implementation of data protection guidelines.

### General meetings of the European Data Protection Board

In 2019, the FDPIC attended two general meetings of the European Data Protection Board (EDPB) to discuss Schengen-related matters, as well as the last general meeting of 2019 at which general information was shared. The EDPB, which was created under the GDPR, held 12 general meetings in all in 2019. As an observer at the general meetings, our participation was confined to Schengen-related issues. For the first time since the EDPB was founded, we took part in two general meetings and had the opportunity to present our stance on national responsibilities, together with other data protection authorities. At the start of December 2019, the Commissioner was also invited by the Board to present a summary of his supervisory procedure against the Geneva-based Libra Association (see Focus 2 ‘Libra project’).

### European Working Party on Privacy Case Handling

A representative of the FDPIC attended the 31st annual European ‘Case Handling Workshops’.

The new European Data Protection Supervisor, Wojciech Wiewiórowski, hosted the 31st annual European Case Handling Workshop on 28 and 29 November, in Brussels. The workshop was attended by the staff of 28 EU and non-EU data protection authorities, including an FDPIC representative.

The workshop was an opportunity to share experiences of investigating complaints, consultancy for data controllers, and the enforcement of data protection laws. Cases from a total of six areas were discussed during the two-day workshop: use of IT service providers by public institutions; handling of manifestly unfounded or excessive requests pursuant to Article 57(4) GDPR; handling of cases pursuant to Article 56(2) GDPR (additional local competence, alongside a lead agency); assessing requests for prior consultation in accordance with Article 36(3) GDPR; credit information systems and data brokers; exercising investigative and corrective powers and weighing up alternative options pursuant to Article 58 GDPR.

### Sub-Working Group on “Border, Travel & Law Enforcement”

We attended the seven meetings of the “Border, Travel & Law Enforcement” (BTLE) subgroup over the course of the year under review. The subgroup carefully monitored the Third Annual EU-US Privacy Shield Review and continues to support this umbrella agreement, which sets out a framework within which law enforcement authorities can share personal name record (PNR) data. “Border, Travel & Law Enforcement” (BTLE) is a sub-working group created by the former “Article 29” Working Party on data protection. The subgroup’s task is to monitor legislative developments affecting the areas of policing, borders and criminal justice, in particular those falling within the Schengen acquis. In this context, it prepares opinions and positions which are then adopted by the European Committee.

The subgroup has focused in particular on the future of surveillance models in the EU’s large-scale IT systems in the area of justice and internal policies. It has examined the drafting of new rules of procedure.

Furthermore, it has focused especially closely on the third annual review of the functioning of the EU-US Privacy Shield. The group has closely monitored the work on the Additional Protocol to the Convention on Cyber-crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, and prepared a Common Position for the Octopus Conference.

It continued monitoring the “umbrella agreement” which regulates the sharing of personal data in police and judicial matters by limiting the rights of US administrations when processing European data, and the establishment of a European framework for sharing PNR data with third countries and for the use of PNR data for law enforcement purposes.

## European General Data Protection Regulation

The new European General Data Protection Regulation (GDPR) also applies, in certain situations, to the processing of data by Swiss companies. The FDPIC attended a number of international conferences and was thus able to join in debates on the challenges involved in applying the new European regulation. More than a year after its entry into force, numerous questions remain unanswered, particularly with regard to the territorial scope.

Adopted on 27 April 2016, the European General Data Protection Regulation (GDPR) has been directly applicable in all Member States of the European Union since 25 May 2018. However, its ambit is far wider than just the territory of the European Union: in offering goods or services to persons located in the European Union, or monitoring the behaviour of those persons – in particular in order to analyse their preferences – data controllers (or processors) become subject to the requirements of the GDPR even if they are not based in the European Union. Throughout the year under review, the FDPIC attended a number of international conferences which enabled him to join in the debates on the achievements and challenges involved in implementing and applying this key text. The Regulation’s extraterritorial scope and the cooperation mechanisms were also raised. As the European French-speaking authorities which are not members of the European Union are faced with the same difficulties, they held meetings throughout the year to discuss the entry into force of the GDPR and to

share their experiences and pool the questions put to them, in order to coordinate their responses.

The FDPIC continued to attend numerous information sessions held on this subject by the federal administration and by private-sector bodies. In his advisory role, he has also answered a great many oral and written questions from the general population and the media.

More than a year after the GDPR entered into force, the European Data Protection Board (EDPB) – the independent European body which helps ensure the consistent application of data protection rules within the European Union – published its guidelines on the territorial scope of the GDPR. This followed a public consultation held to discuss these guidelines, attended by the FDPIC in collaboration with the Monegasque data protection authorities (CCIN – Commission de contrôle des informations nominatives), to seek clarification of a number of aspects of this extremely important issue for third countries that are part of the EU landscape. A meeting was also held in Bern, in February 2020, to analyse this new version. Information about the application of the GDPR is regularly updated on our website.

## Brexit and transfer of personal data

Following the UK referendum on leaving the EU (Brexit) in June 2016, the British government notified the EU of its decision. After a number of delays, the UK's departure took place on 1 February 2020.

As outlined in the last activity report, the FDPIC attended numerous meetings with authorities of the Confederation and the UK to make sure that the free movement of personal data between Switzerland and the UK can continue after Brexit. The UK is considered as a country to afford an adequate level of protection, and the FDPIC currently sees no cause to alter that status.

The EU will decide by the end of 2020 whether it still deems the UK to offer an adequate level of data protection. The FDPIC is actively monitoring these developments.

## Consultative Committee on Convention 108 (T-PD)

The T-PD has adopted guidelines on artificial intelligence and data protection.

These guidelines are designed to help political decision-makers, developers of artificial intelligence, manufacturers and service providers to ensure that AI applications do not breach the data protection rights. They make reference to major issues already picked up in the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. The Committee also adopted an opinion on the draft Recommendation of the Committee of Ministers to member states on “the human rights impacts of algorithmic systems”, submitted for comments by the Steering Committee on Media and Information Society.

It decided on the Committee's work programme for 2020–2021, which will include, in particular, monitoring the modernisation of the Convention, promoting the Convention, a specific recommendation on facial recognition, the processing of personal data in education systems, and a review of profiling. It is also working on monitoring and evaluation mechanisms for Convention 108+ and decided to form a working party comprising members of the Board and any interested delegation, which will be tasked with drawing up further proposals for the new mechanism.

## Adequacy decision on Switzerland's level of data protection

The European Commission has continued its review process for the adequacy decision on Switzerland, which was first made in 2000. It should be publishing its findings in May 2020. Maintaining this decision is a priority of the Federal Council.

An adequacy decision is a decision made by the European Commission, establishing that a third country's internal legislation or international commitments afford an adequate level of personal data protection comparable to that guaranteed in the European Union. An adequacy decision enables personal data to circulate securely between the European Economic Area (EEA) and the third country concerned, without specific guarantees having to be introduced by the data controllers themselves.

Under Article 45 paras. 3 and 4 of the GDPR, the European Commission monitors developments affecting the level of data protection in third countries which, like Switzerland, are the recipients of a decision on the adequacy of protection.

All third countries which benefit from an adequacy decision will be evaluated according to the same methodology. In particular, the Commission must take into account the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and proper functioning of one or more independent supervisory authorities, and the international commitments made by the third country. The signing of Convention 108+ in November 2019 and the revision of the FADP will be important factors in upholding the decision – which is one of the Federal Council’s priorities (see Interpellation 17.4088).

The review process officially commenced in March 2019, and will continue with regular discussions until the spring of 2020. Throughout the year under review, the FDPIC participated in the working party led by the Federal Office of Justice (FOJ). The European Commission has until 25 May 2020 to publish the findings of its evaluation and renew the decision on Switzerland. Under the GDPR, adequacy decisions remain valid until they are amended, replaced or repealed.



# Libra Project

The cryptocurrency project Libra has created quite a stir in the media and among data protection agencies the world over. In a preliminary procedure, the FDPIC affirmed his competence as the supervisory body for the data processing undertaken by the Geneva-based Libra Association, and demanded the relevant documentation. The Libra Association assured the FDPIC that it would implement the measures necessary to protect privacy.

The FDPIC was alerted by media reports to the Libra Project, the planned worldwide cryptocurrency under the auspices of Facebook. In particular, he took note of the comments made by Vice President for Messaging Products at Facebook, David Marcus, at the hearing of 16 July 2019 before a US Senate committee on the Libra Association's crypto project as well as on the leadership function of the Libra Association and the role of the FDPIC as its supervisory authority.

As the FDPIC had not been contacted beforehand by the project's promoters, he wrote to the Libra Association in Geneva on 17 July 2019. In that letter, he informed the Association that he had taken note of the comments by David Marcus to the effect that data protection would be fundamental to the project. At the same time, the FDPIC made it clear that, when personal data are to be processed,



he expects a risk impact assessment which, among other things, describes the proposed data processing actions, evaluates the privacy risks to data subjects, and lists the targeted measures to mitigate those risks.

Moreover, he asked the Libra Association to submit to him documents about the current status of the project.

After the Libra Association promptly submitted the requested information about the Libra Project to the FDPIC, on 17 September 2019 a personal meeting took place between the FDPIC and representatives of the Libra Association in Bern. The Libra Association confirmed that it was developing a globally consistent data protection standard for the system which, in particular, will satisfy the requirements of the EU's General Data Protection Regulation. This is consistent with the stance of the Commissioner, who is insistent upon a high level of protection for users' personal data. The Association also affirmed that, in order to satisfy the privacy-by-design principle, the FDPIC would be involved in its ongoing development work at an early stage.

The Libra Association gave the FDPIC a written assurance that it would take the measures necessary to create the uniform data protection standard and appoint a data protection office in good time before launching the currency, and that the latter office would be tasked with producing a risk impact assessment. In a letter dated 17 February 2020, the Libra Association informed the FDPIC that the associated work is still ongoing. Moreover, it reaffirmed that it will implement the measures promised to the FDPIC to protect privacy in the Libra Project.

Since announcing his competence to supervise the Libra Project, the FDPIC has been conducting discussions with colleagues at the EU data protection authorities and regularly updates the EU Board on the project. Furthermore, on 23 August 2019 a meeting led by the Swiss State Secretariat for Economic Affairs (SECO) was held with the US House Committee on Financial Services, at which the Commissioner shared information about the status of his supervisory procedure (see below). The Commissioner is also in contact with the Swiss National Bank and FINMA to coordinate the activities of the federal agencies involved and ensure that information is shared. FINMA has promised to keep the Commissioner updated on the procedure pending before it for the issue of a banking licence. This will enable the FDPIC to coordinate the timing of his procedure.

As always, the FDPIC will continue sharing updates on relevant developments in the supervisory procedure with the global public.

## International activities and meetings

Together with other federal authorities, on 23 August 2019 the FDPIC took part in an event in Bern, organised by the State Secretariat for International Financial Matters, to which six members of the U.S. House Committee on Financial Services were invited, led by their Chair Maxine Waters. They were particularly interested in regulatory oversight of the activities of the Geneva-based Libra Association, and the legal parameters for cryptocurrencies in Switzerland, as well as their potential impact on the personal rights of data subjects in the USA. The Commissioner gave the delegation a summary of the pending supervisory procedure against the Libra Association, and clarified any aspects that were unclear to them.

The Commissioner explained that, like all other data protection authorities, he is affected by the Libra project and its global network and is seeking to support the global community of data protection authorities in their joint efforts to protect the general public. Therefore, he was liaising closely with the European Data Protection Board (EDPB) and the Global Privacy Association (GPA, at the time still called the ICDPPC) and other data protection authorities. He particularly stressed the fact that the Swiss procedure would in no way prejudice or affect the competences and powers of the other data protection authorities in other countries. He also said he would prevent any attempts to pit individual data protection authorities against each other. He informed the chairs of the EDPB and the GPA that he would continue to share brief updates with them about the procedure in Switzerland.

A representative of the EDPB subsequently took part in a panel on data protection at the 'Conference on global stablecoins' organised by the Bank for International Settlements on 16 September 2019, in Basel. Most of the participants were representatives of central banks and financial regulatory authorities, and the event was the first opportunity of its kind to raise and discuss data protection aspects.

The Commissioner liaised on a number of occasions with representatives of the GPA and the EDPB. At the International Conference of Data Protection and Privacy Commissioners in Tirana (see chapter 1.9), the FDPIC had the opportunity to meet in person with the data protection commissioners of various European countries, as well as the US Federal Trade Commission. The Commissioner also liaised with representatives of the Swiss National Bank and the Swiss Financial Market Supervisory Authority (FINMA), who assured him that his agency would be kept up-to-date of the progress over time of financial authorisation procedures concerning the Libra Association. In addition, on 3 December 2019 the Commissioner attended a meeting of the European Data Protection Board in Brussels, at which information was shared (see chapter 1.9).





# Freedom of Information

## 2.1 General

Ever since the Freedom of Information Act came into force, there has been no let-up in the paradigm shift, and the principle of freedom of information is being successfully applied by the majority of federal authorities. This observation is backed up by the figures given below, which confirm the trend of recent years: in most cases, full access is granted to the requested documents, and there is a marked increase in the number of requests for access (see chapter 2.2).

An impressive 61 percent of cases were settled with an amicable outcome in 2019, the clearest indicator yet of how effective oral media sessions are. We must continue encouraging this as the preferred approach. As well as granting applicants swift access to information, a number of agreements also enabled applicants to engage in direct dialogue with the administration and, in some cases, forge close ties for future collaboration with the federal authorities.

Depending on the specifics of each case, completing mediation procedures within the statutory 30-day time limit remains challenging. This is particularly true of complex procedures involving three or more parties, concerning access rights to documents with information related to trade secrets or documents about protecting the privacy of private individuals or government employees. Since these mediation procedures often involve extensive and, at times, complex clarification work with the parties involved, the procedures take longer to complete (see chapter 2.3).

The Freedom of Information Act again proved invaluable in promoting transparency, information and control for the public in 2019. Therefore, we must remain vigilant and ensure it is not derailed by the introduction of new legal provisions designed to exclude its application. During the year under review, some parts of the administration (such as the Federal Customs Administration and the Federal Office of Public Health) again stepped up their efforts to exempt areas of their activity, or certain categories of document, from the principle of freedom of information in administration (see chapter 2.4). In contrast, the reaffirmation of transparency in the Federal Act on Public Procurement (PPA) in June 2019 and the decision by the Political Institutions Committee of the National Council on the principle of exemption from charges for requests for access are evidence of the federal legislature's commitment to the principle of freedom of information.

Unfortunately, the Federal Council objected to the transparency enshrined in the PPA and, in its implementing provisions for the Act, has now restricted some aspects of that transparency (see chapter 2.4).

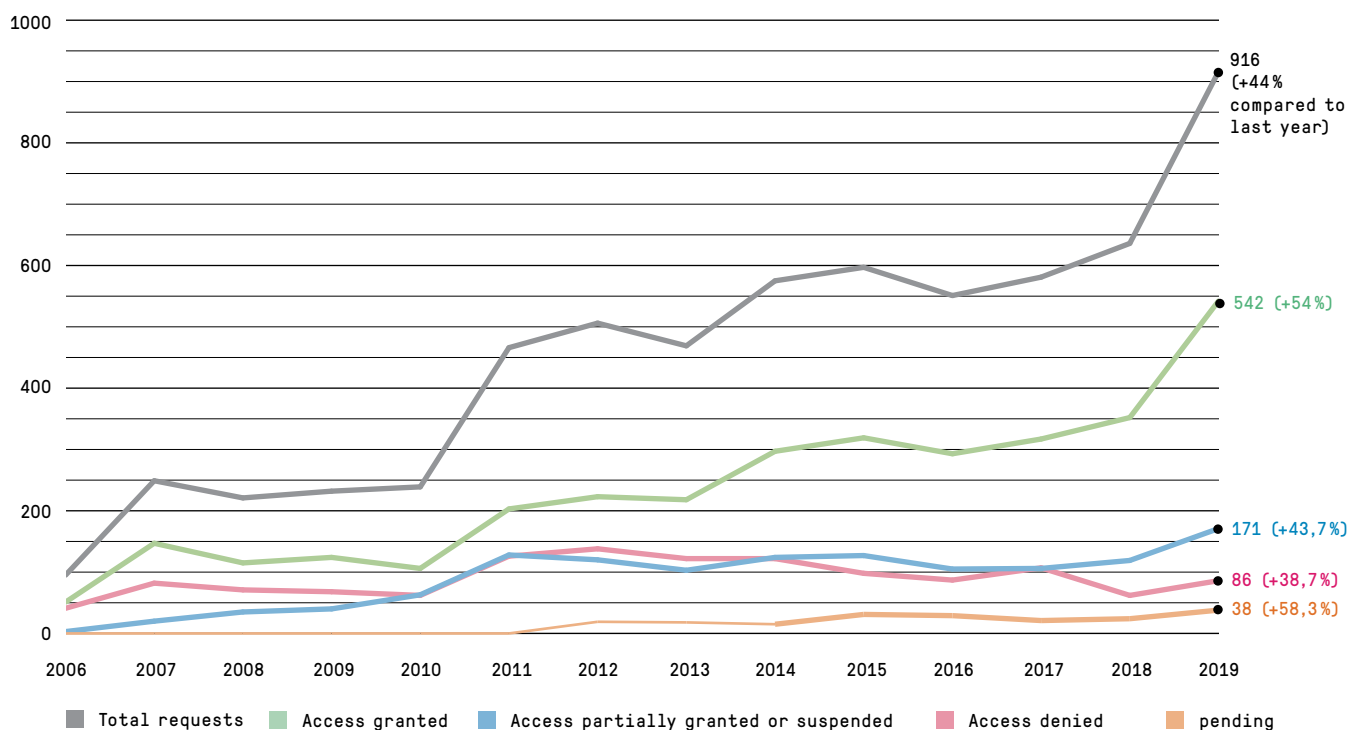
## 2.2 Requests for access – further increase in 2019

According to figures provided by the federal authorities, 905 requests for access were submitted to them in 2019, compared with 636 in 2018. This increase can be partly explained by the fact that the FOSPO alone received 175 requests for access. Including the Office of the Attorney General of Switzerland (10) and the Parliamentary Services (1), the total is 916 (or 44 per cent more than in 2018). Growing public awareness over the years of the principle of freedom of information, due not least to media coverage, is undoubtedly a contributing factor as more people take up the opportunities this principle presents. This trend is likely to continue over the next few years, particularly as we are seeing

more and more calls by the general public for transparency in government and politics. The authorities granted full access in 542 cases (59 per cent), compared with 352 in 2018, or 55 per cent. Moreover, in 171 cases (19 per cent), applicants were granted partial access to documents. In 86 cases (9 per cent) they were completely denied access (compared with 62 in 2018, or 10 per cent). The authorities indicated that 38 requests for access were withdrawn (compared with 24 in 2018, or four per cent), 43 requests were still pending at the end of 2019, and in 36 cases there was no official document. Since 2015, full access has been granted to the requested documents in more than 50 per cent of cases. By comparison, the

number of requests for access denied outright remains small and has stabilised over the years at around 10 per cent. The Commissioner notes a growing tendency towards transparency among government authorities. The transparency measures taken by a number of federal authorities have contributed to the increase in the number of requests for access granted and are consolidating the paradigm shift sought by the federal government (see the detailed statistics in chapter 3.3).

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



**Federal departments and federal offices**

The figures notified by the federal offices reveal that the FOSPO received the most requests for access in 2019 (175), followed by the FOEN and the FOPH, with 35 requests each, then SECO (34). The departments which received the most requests are the DDPS (225) and the FDHA (168). Conversely, ten authorities informed us that no requests for access were submitted to them during the year under review. The Commissioner himself received ten requests. He granted full access in six cases. In one case, the requested document did not exist, and in three cases the requests were withdrawn.

In 2019, fees charged for obtaining access to official documents totalled CHF 18 185. Although this is a higher total than in 2018 (CHF 13 358), it is still not out of the ordinary compared with previous years.

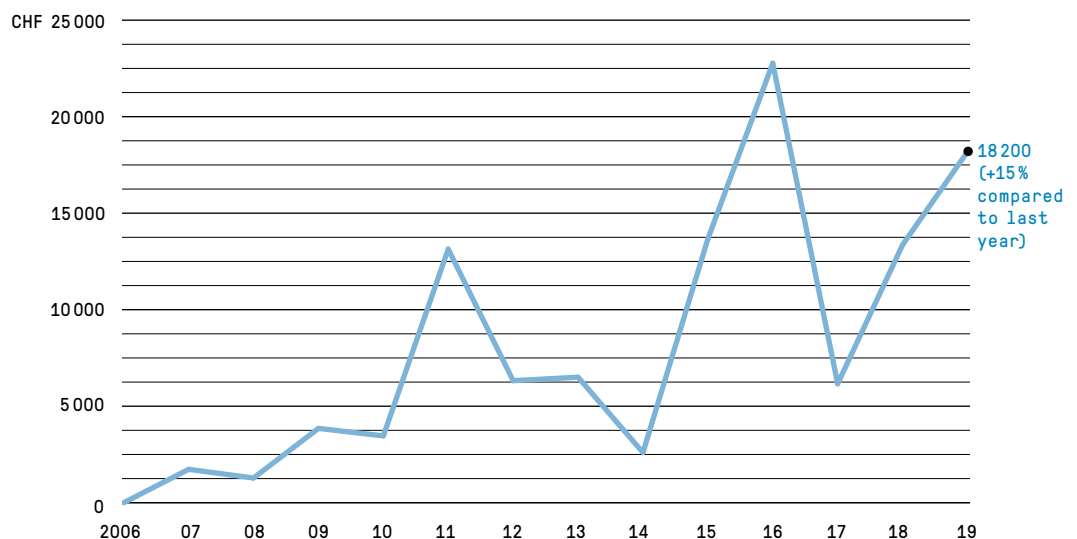
Whereas the FDJP and the Federal Chancellery did not charge any fees, the other six departments did invoice applicants for some of the time spent dealing with their requests (FDHA: CHF 8710; DDPS: CHF 300; FDF: CHF 3750; EAER: CHF 700; DETEC: CHF 2750). It is important to note that just 31 out of 916 requests for access incurred a fee. Whilst this figure is higher than in 2018, when just 17 requests incurred a fee, the number of requests for access was also much higher. As in previous years, fee-charging is the exception, as access was granted free of charge in nearly 97 percent of cases. Nevertheless, the Commissioner notes that the federal authorities tended to charge smaller fees, but on a more regular basis during in the year under review.

In the context of the implementation of the Graf Litscher initiative (16,432 n lv. pa. Graf-Litscher).

Principle of freedom of information in the administration. Ensuring predominantly free access to official documents), the Political Institutions Committee of the National Council observed that some departments had already invoiced several thousand francs, robbing the principle of access to official documents of its substance. The Committee therefore feels it is appropriate to enshrine in law the principle of free access, and has issued the revised Freedom of Information Act for consultation. To this end, on 14 February 2020 it submitted for consultation a proposal for a change in the law.

As regards working hours spent processing requests, the Commissioner reiterates that the authorities are under no obligation to record those hours and there is no directive on a standard recording procedure for the whole of the federal administration.

**Figure 2: Fees charged since the FoIA entered into force**



Details are sent to the Commissioner on a purely voluntary basis and only partially reflect the working hours actually spent handling requests. According to these data, the working hours published this year were 4375 hours, which is less than in 2018 (4827 hours). This decrease is mirrored in working hours devoted to preparing for mediation sessions, which totalled 473 hours (compared with 672 hours in 2018 and 914 hours in 2017). This low number of hours is at odds with the net increase in the number of mediation procedures. In all likelihood, not all the time spent preparing for procedures has been recorded. Moreover, in many cases time spent drafting a ruling or on appeal proceedings was not notified to the Commissioner.

#### **Parliamentary Services**

The Parliamentary Services informed us that they received just one request for access, which was denied outright.

#### **Office of the Attorney General of Switzerland**

The Office of the Attorney General of Switzerland notified us that it received ten requests in 2019. Access was granted in three cases and denied outright in one case. As for the remaining cases, there was no official document in two of them, three were withdrawn, and the final one is still pending.



## 2.3 Mediation procedure – significant rise in mediation requests

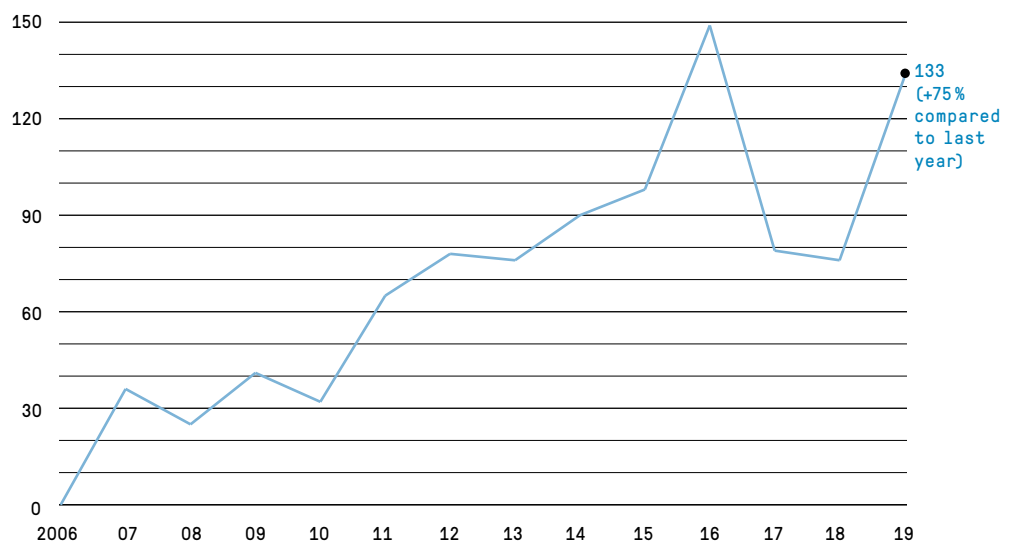
In 2019, 133 mediation requests were filed with the Commissioner, which is 75 percent more than in 2018 (76). The media (34), private individuals (40) and companies (47) were filing the majority of requests. From these figures, we can deduce that, of the 258 cases in which the federal administration fully or partially denied access, 132 were a request for mediation to the Commissioner. These account for 51 percent of all unmet requests for access. This increase in the number of requests for mediation can be partly explained by the need to consult numerous third parties regarding one request for access.

28 of those third parties then filed requests for mediation with the Commissioner following the consultation. It should be pointed out that this rise in the number of requests generates a large volume of work, and had a significant impact on the Commissioner's workload. 108 mediation requests were settled in 2019, 93 of which were submitted during that year and 15 of which had been submitted in 2018.

In the majority of cases (48), the participants were able to reach a consensual solution. The Commissioner also issued 26 recommendations, enabling him to close 31 cases which were unlikely to result in agreement between the parties.

The cases dealt with included six mediation requests that were withdrawn without the Commissioner's intervention, eight cases which did not satisfy the conditions for the application of the Freedom of Information Act, and twelve requests which were not submitted on time. At the end of the year, four mediation procedures had been suspended at the participants' request.

**Figure 3: Mediation requests since the FoIA entered into force**



## Duration of mediation procedures

The table below is split into three sections, depending on how long it took to settle the procedures. It shows that, in 2019, the majority of procedures were concluded within the 30-day period. It should be pointed out that the processing time does not take account of the period during which a mediation procedure is suspended with the participants' consent. Most notably, a mediation procedure is suspended when an authority wishes to re-examine its position after the mediation session, or has to consult the third parties involved.

Failure to meet the deadline is often due to unavailability of the people or authorities concerned (holidays, illness, travel), the large number of third parties involved in the procedure or the need to resolve complex legal issues. These explanations also apply to the four cases (including three procedures which were consolidated) which took longer than 100 days to process. 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 impossible to meet deadlines. It should be noted that the above-mentioned situations fre-

quently 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.

A comparison with previous years reveals that, since the pilot was conducted in 2017, the processing time for mediation procedures has decreased substantially. The figures for 2019 clearly confirm this significant reduction and, when correlated with the proportion of amicable outcomes, they demonstrate the effectiveness of the measures taken, in particular the emphasis on oral mediation.

In most cases, the statutory 30-day deadline for completing the mediation procedure can be met. This is provided the mediation sessions are held according to schedule, i.e. without the parties requesting any postponements, and culminate in agreement within the deadline from receipt of the request. If no agreement is reached, the written recommendation cannot always be issued to the parties involved within 30 days of receipt of the request. By contrast, if a large number of mediation requests are submitted within a short period, a lack of resources means that the deadline cannot be met. If there is already a backlog with the processing of mediation procedures,

each new request received only compounds this. In complex cases and in procedures involving a number of parties (i.e. several third parties), the 30-day deadline is also excessively tight. Moreover, experience shows that the involvement of legal representatives by third parties being interviewed at the access and mediation procedure stage is not conducive to a straightforward, pragmatic and swift solution.

Table 1: Processing time of mediation procedures

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

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

### Proportion of amicable outcomes

The ratio of recommendations to amicable outcomes is the best measure of the effectiveness of the measures introduced in 2017 and of mediation sessions. There are numerous advantages to amicable solutions. For instance, they are an opportunity to clarify the facts, accelerate the procedure for access to documents, or establish the bases for possible future collaboration among the participants in the mediation session. Over the year under review, 48 amicable outcomes were achieved and 26 recommendations were issued by the Commissioner to settle 31 cases. Therefore, the ratio of recommendations to amicable outcomes is 61 percent.

The Commissioner notes that the proportion of mediation procedures culminating in an amicable outcome has risen further.

Table 2: Amicable outcomes

2013–2016	40%
2017	60%
2018	55%
2019	61%

### Number of pending cases

The figures below show the number of pending cases at the end of the year under review. As at January 2020, the number of cases still pending from 2019 stood at 43, including four suspended procedures.

It should be noted that 42 mediation requests were filed during November and December, and 40 of them had been settled at the time of going to press. However, although much higher than previous years, the number of pending cases is the logical consequence of the sharp increase in the number of mediation requests and of the limited resources at the Commissioner's disposal. If no additional resources are forthcoming, there is a considerable risk that processing times will steadily increase, that the deadline can no longer be met, and that there will be a further rise in the number of pending cases at the end of next year.

Table 3: Pending mediation procedures

End of 2016	33
End of 2017	3 (2 in process; 1 suspension)
End of 2018	15 (13 completed in February 2019; 2 suspended)
End of 2019	43 (40 completed by the time of going to press; 3 suspended)



## 2.4 Office consultations

### Office consultations on the draft of a law on customs and border security; opening of the consultation process

The FCA wants to exclude key areas of its activity from the Freedom of Information Act. This is what it is proposing in the draft for a new federal law on customs and border security (BBZG). In his opinion as part of the office consultation, the Commissioner objected to these plans.

Among the FCA's proposals was a provision that allows the authority to obtain "voluntarily supplied data of private individuals". According to the explanatory report, these "voluntarily supplied" personal data should be subject to special confidentiality, pursuant to Art. 7(1)(h) of the FoIA. In particular, these data should be processed in order that respective economic operators can be allowed to simplify procedures in additional ways.

In his opinion, the Commissioner pointed out to the FCA that three requirements must be met cumulatively in order for the aforementioned exception to apply: Firstly, the information must have been shared by a private individual. Secondly, it must have been voluntarily and spontaneously shared. If the information was disclosed in fulfilment of a legal or contractual obligation, this does not constitute voluntary sharing. Thirdly, the authority must have given an assurance of confidentiality at the express request of the informing party. The authority may not offer such assurance of its own accord, and may not offer it recklessly. In light of the promised procedural simplifications by the FCA, the Commissioner already

had misgivings as to whether the criterion of voluntary disclosure was met. Moreover, the assurance of confidentiality may only be given at the request of the private individual, and then only in individual cases. Authorities cannot give a proactive, general assurance. After all, in its dispatch on the Freedom of Information Act, the Federal Council itself explicitly stipulated that to do otherwise would undermine the very purpose of the Act, which is to facilitate public access to official documents and promote transparency in administration.

The FCA's proposal thus contradicts the spirit and purpose of the Freedom of Information Act and the exception clause in Art. 7(1)(h) FoIA.

Furthermore, the draft provided for an obligation of secrecy whereby people responsible for, or involved in, enforcing this Act must observe secrecy towards other authorities and private individuals concerning the observations made in the performance of their duties, and must deny access to official documents. The FCA's perception is that this far-reaching obligation of secrecy applies similarly to the Vehicle Duty Act, the Mineral Oil Tax Act, and the Alcohol Act. According to the FCA's explanatory report, nowadays many requests for access are received which do not relate to government activity. Instead, they are merely fishing for sensitive economic data of third parties. What the FCA fails to recognise is that the legislator has already safeguarded protection of sensitive "economic data" in the Freedom of Information Act. Thus such commercial information already enjoys extensive protection under Art. 7(1)(g) FoIA (professional, business or manufacturing secrets). If there is

established evidence of such secrets, these documents can be redacted or, if this is not possible, removed entirely from access. Moreover, the companies concerned can take legal action against government plans to grant access. There are many years of Federal Supreme Court rulings to support this.

Furthermore, with its comprehensive reservation as to confidentiality, the FCA is disregarding the legislator's clear intent, which is that the Freedom of Information Act should promote transparency with regard to the administration's mission, organisation and activities. In fact, the legislator's explicit intention in introducing the principle of freedom of information was for the general public to submit requests for access, not least in order to keep a check on the authorities' dealings with third parties. Thus another objective of the principle of freedom of information is to prevent mismanagement and corruption in government. Indirectly, therefore, it also protects individual areas of the federal administration against potential accusations of having made secret agreements or engaged in dishonest practices with economic operators to the detriment of others, or at taxpayers' expense.

The Commissioner also pointed out to the FCA that unwanted requests for access or any additional workload are not, on their own, sufficient or cogent arguments for demanding a sweeping secrecy obligation.

For these reasons, the Commissioner demanded in the office consultation that the FCA drop its transparency-hostile proposal for such a secrecy obligation, for all of the laws concerned.

Based on feedback from the authorities consulted, the FCA revised the draft and undertook a second office consultation. In the revised draft legislation, the provision concerning the secrecy obligation for people responsible for enforcing the law was dropped and a number of parts of the explanatory report were modified. Otherwise, however, the FCA stuck to its plan.

At the time this report was finalised, the FDF had yet to make a decision on the next steps. If the Federal Council and Parliament were to align with the FCA, this would result in whole swathes of the FCA's primary statutory duties being excluded from freedom of information.

### **Consultations on the agreement between the Confederation and the cantons concerning the harmonisation and sharing of police technology and IT systems**

*In an agreement between the federal government and the cantons concerning the harmonisation and sharing of police technology and IT systems (VPTI Switzerland), the Conference of Cantonal Justice and Police Directors (CCJPD) incorporated a choice of law clause according to which, where police technology and IT systems are concerned, the laws of the canton of Bern apply to freedom of information in government, rather than the federal Freedom of Information Act.*

The CCJPD established the programme to harmonise Swiss police information (HPI) in 2010. An administrative office that is part of the Swiss Competence Centre for police technology and information technology (PTI) was charged with the operational implementation of the programme. Now, the HPI and PTI business areas are to be governed by a single agreement between the Confederation and the cantons. The draft of this agreement included a choice of law clause which stated that all the cantonal and federal authorities involved are subject exclusively to the laws of Bern on public information, in matters including freedom of information in government.

Early in the reporting year, during a preliminary consultation by the Federal Office of Justice (FOJ), the Commissioner made it plain that the proposed choice of law clause, insofar as it affects federal authorities, circumvents the Confederation's Freedom of Information Act and, as such, is in violation of federal law. Thus it is also in breach of Art. 48(3) of the Federal Constitution, which stipulates that agreements between cantons must not be contrary to the law, to the interests of the Confederation or to the rights of other cantons.

During a later consultation, the Commissioner made the observation to the CCJPD that, whilst the comments he made to the FOJ have been incorporated in the clarifications on the agreement, the choice of law clause in the draft agreement remains unchanged. Thus, according to the wording of the choice of law clause, the laws of the Canton of Bern continue to apply to the federal authorities involved in the agreement, including with regard to freedom of information in government, data protection or procurement. The Commissioner stated to the CCJPD that, not least to establish legal certainty in the agreement, the reservation of the applicability of the Federal Freedom of Information Act to federal authorities must be stated in the agreement itself and not just in the clarifications, which – as experience shows – are only read if a particular standard is unclear. Lastly, the Commissioner noted that, irrespective of the involvement of one or more federal authorities in the planned agreement, said authorities must still be subject to the Confederation's Freedom of Information Act insofar as they produce documents or

are the primary recipients of documents. In other words, when federal authorities are assessing requests for access to official documents concerning the harmonisation and sharing of police technology and IT systems, they must be guided not the laws of the Canton of Bern on public information, but solely by the Confederation's Freedom of Information Act.

### **Office consultation on a single point of orientation for official documents**

[The Swiss Federal Archives \(SFA\) asked the Federal Council to conduct a study as a basis for decisions on a single point of orientation for official documents. The Commissioner's clarifications were incorporated in the request to the Federal Council.](#)

In 2008, the Federal Council decided to introduce GEVER and to establish a single point of orientation (SPO) for official documents in the federal administration. The SPO was to use metadata from the GEVER electronic records and process management system to produce a catalogue. The search results in this SPO were also to be used by applicants under the Freedom of Information Act to make specific requests for access. In 2012, the SFA developed and trialled a pilot web application for this purpose. The project was twice put on hold. At the end of 2019, the SFA had to present an update to the Federal Council and make a proposal for the next steps. The Commissioner commented on the SFA's proposal for a "single point of orientation for official documents" during an office consultation.

A single point of orientation, complete with metainformation, would be conducive to upholding the principle of freedom of information and help ensure transparency in government. Therefore, the Commissioner welcomes these efforts.

In his opinion to the SFA, he pointed out the importance of making a clear distinction in the SPO project between the Freedom of Information Act and the authorities' general duty of information. Art. 21 of the Freedom of Information Act (FoIA) contains an implementing provision on information about official documents. However, rather than establishing an independent legal basis, it merely fleshes out the authorities' existing general duty of information.

A single point of orientation for official documents is a tool used by the authorities to proactively share information: according to the Constitution and the system of government and administration, the authorities already have a general duty to voluntarily share information about their functions and key business, and to disseminate suitable information about these (active information sharing). By contrast, the Freedom of Information Act comes into play when somebody submits a request for access to an authority (passive information sharing).

At its meeting of 6 December 2019, the Federal Council decided to conduct a study into the creation of a central register of official documents. Among other things, the study will investigate how such a system could be implemented, the technical solutions, and the responsibilities within the federal administration. The findings of the study are due to be presented at the end of 2020.

## Office consultation on the CAR-T cell therapy charging arrangement

The Federal Office of Public Health (FOPH) proposed adopting a resolution that would exempt tariff approval for autologous CAR-T cell therapy from the Freedom of Information Act. The Commissioner opposed this.

The FOPH proposed to the Federal Council that it should approve the charging arrangement between hospitals and health insurers (contracting partners) concerning autologous CAR-T cell therapy. This arrangement contains a confidentiality agreement under which, aside from the contracting parties, the agreed variable amounts reimbursed for autologous CAR-T cell transplants may only be disclosed to the approving authorities and the relevant health authorities in the patient's home canton. One of the FOPH's arguments was that the amount reimbursed is a business secret. It also proposed that the submission to the Federal Council and the reimbursement agreements listed in the Enclosure should remain excluded from the right of access under the Freedom of Information Act, even after the charging arrangement has been approved by the Federal Council.

During the office consultation, the Commissioner first of all pointed out to the FOPH that, under the Freedom of Information Act, health and accident insurers are deemed to be authorities for the purposes of compulsory insurance. Since the information provided to the FOPH by third parties for tariff approval purposes is based on the law (Federal Act on Health Insurance), such a confidentiality agreement in a charging arrangement is not legally permissible, nor can it be approved by the Federal Council. Moreover, the Commissioner noted that the Freedom of Information Act already safeguards both the protection of business secrets and the protection of privacy, eliminating the need for an exception to the Act. He further explained that the signed submission to the Federal Council is part of the joint reporting procedure and, as such, already excluded under Art. 8(1) FoIA from the right of access under said Act, unlike the enclosures attached to it.

For the sake of completeness, the Commissioner also pointed out that there is no cause to apply Art. 8(3) FoIA, as the charging arrangement and the associated reimbursement agreements were drawn up before the office consultation commenced, and thus do not count as documents in this procedure (the Commissioner has previously commented on the same matter, see 26<sup>th</sup> Activity Report, Section 2.4). Whereas Art. 8(3) FoIA does allow the Federal Council, in exceptional cases, to decide against allowing any access to official documents submitted to the office consultation procedure, it must base its considerations on the reasons for exceptions laid down in the Freedom of Information Act.

In particular, the Commissioner drew the FOPH's attention to the fact that the Freedom of Information Act does not entitle the Federal Council to arbitrarily limit the scope of application of said Act and, circumventing due legislative process, adopt a resolution excluding official documents from its scope of application.

The FOPH subsequently modified the submission to the Federal Council. However, just a few weeks later, it issued a fresh demand for a specific exemption from the Freedom of Information Act and proposed a partial amendment to the Health Insurance Act to that effect (see below).

## **Office consultation on the consultative process for the partial amendment of the HIA regarding cost-containing measures – Package 2**

The Commissioner objected to the Federal Council's plan to introduce an exception to the freedom of information principle for documents concerning pricing models for drugs in health insurance.

During an office consultation, the Federal Office of Public Health (FOPH) proposed, among other things, that records concerning the amount, calculation method and modalities of pricing models and reimbursements in compulsory health insurance should be excluded from access. When setting the prices of drugs on the specialities list (SL), pharmaceutical companies – as the marketing authorisation holders – can negotiate discounts with the health insurers (referred to as pricing models). In pricing models, the official price on the SL differs from the actual price which the health insurer must pay to the pharmaceutical company (reimbursement).

Under its plans, the Federal Council wants to exempt all records relating to pricing models from the scope of application of the Freedom of Information Act. The agreed discounts and the full reimbursement mechanism would then not be disclosed to the general public. The Federal Council takes the view that, if the actual prices were publicised, the pharmaceutical companies would no longer be willing to negotiate such pricing models.

Furthermore, the Federal Council also argues that the majority of requests for access relating to documents about drugs on the specialities list are not made by members of the public who are seeking information about government actions. Rather, they originate chiefly from pharmaceutical companies requesting an insight into business information of competing companies. The counter-argument to this is that competitors too have a legitimate interest in being able to review the FOPH's licensing practices for competing products. Business and manufacturing secrets and the privacy of the companies concerned are explicitly protected, even when the Freedom of Information Act is applied.

It is the Commissioner's opinion that the embedding of a confidentiality clause in the Health Insurance Act is a move in the wrong direction. In his opinion given during the office consultation, he reiterated that the Freedom of Information Act is designed to foster understanding of the administration and how it functions, and increase acceptance of government actions. The FOPH increasingly relies on such pricing models as a policy tool. By contrast, there is a widely supported consensus on cost transparency in healthcare, particularly as the constantly rising health insurance premiums have long been cited by the general public as one of their biggest concerns. In this context it is vital for the general public as well as competitors to retain the ability to thoroughly investigate and monitor the FOPH's authorisation practices. In the medium and long term, an active transparency strategy would result in lower prices, particularly on the inter-

national level. In the long run, close cooperation between states is essential for a truly effective pricing policy.

The FOPH did not take account of the Commissioner's concerns. In the near future, the Federal Council will be opening a consultative process on the partial revision of the Health Insurance Act.

## Office consultation on the complete revision of the Ordinance on Public Procurement

While the complete revision of the Ordinance on Public Procurement was being drawn up, a difference of opinion emerged between the Commissioner and the Federal Council with regard to the accessibility of the new list of sanctioned providers.

Swiss Parliament adopted the complete revision of the Federal Act on Public Procurement (PPA) on 21 June 2019 (case no. 17.019). Contrary to the Federal Council's planned full exemption, the freedom of information principle in public procurement remains enshrined in the new draft, as it is in the current PPA.

The Commissioner had strongly advocated this, both during the office consultation procedure and over the course of the parliamentary consultations (see 26th Activity Report 2018/19, Section 2.4). In the first half of the year under review, the FOBL presented the draft of the completely revised related Ordinance during an office consultation. Art. 45(3) of the Act adopted by Parliament introduced a list of sanctioned providers and subcontractors that are designated as "non-public".

The list includes companies that have been legally disqualified from future public contracts because, for instance, they have violated anti-corruption provisions or concluded unlawful anti-competitive agreements. Art. 25(3) of the revised Ordinance provides for a separate right of access to this list solely for the Contracting Authority, but not a general right for the general public to view it.

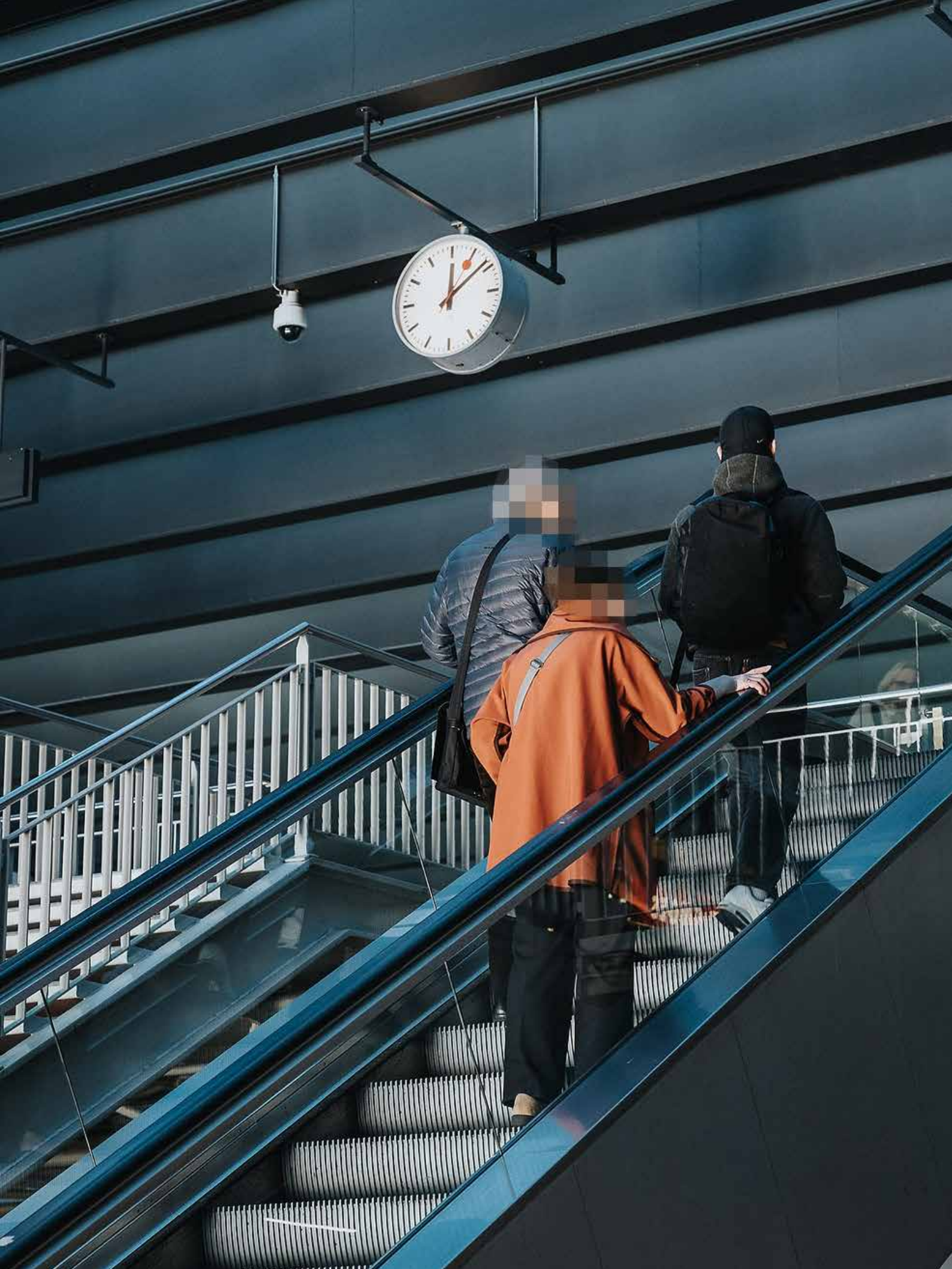
The explanatory report on the Ordinance clarifies that, according to the dispatch on the PPA, there is no right of access to the list under the Freedom of Information Act.

The Commissioner opposed this interpretation during the office consultation: the Federal Council's draft of the revised PPA completely excluded all documents in connection with procurement from the scope of application of the Freedom of Information Act. However, Parliament decided in favour of full transparency in public procurement, and rejected the Federal Council's plans for secrecy. In keeping with the legislator's clear intention of creating transparency, the Freedom of Information Act must therefore apply without restriction to the revised PPA.

Moreover, the Commissioner takes the view that this list's designation as "non-public" in the Act does not warrant it being classed as "secret" under a special provision of Art. 4 FoIA. This would require an explicit, statutory reservation of the Freedom of Information Act in the PPA itself. Rather, "non-public" simply means that the list is not actively published by the authority. The wording of the legal provision in no way implies that the list must be kept secret should a request for access be received.

This difference of opinion could not be resolved. The Federal Council dismissed the Commissioner's objections.

The revised Act and the related Ordinance will come into force on 1<sup>st</sup> January 2021.







# The FDPIC

## 3.1 Duties and resources

### The Commissioner

At its meeting of 10 April 2019, the Federal Council re-elected Adrian Lobsiger for a second term of office (51<sup>st</sup> legislative period), which will run until the end of 2023.

### 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 Data Protection Act (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 Schengen Data Protection Act (SDPA, SR 235.3) already covers an aspect of the complete revision. The SDPA gives our authorities additional duties and powers concerning the processing of police-related personal data, which are particularly sensitive (see 26<sup>th</sup> Annual Report, chapter 2.1).

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. For the first time since 2005, this increased the headcount of data protection staff. These three additional positions were filled by spring 2020, taking the total number of staff at the FDPIC to 27 full-time equivalents.

Owing to the narrow scope of application of the SDPA, the newly recruited staff will focus on our oversight of the Confederation's police authorities. Due to retirements, the Commission's age structure has become younger. As this eases the pressure on the staff budget, it probably allow us to increase our staff numbers further in the next reporting period.

At what point the FDPIC will be able to request and recruit the additional staff promised to implement the complete revision still depends on when the new FADP enters into force. The timing of this remains uncertain. According to Art. 40a of the bill, which has been approved by both chambers of the Federal Assembly, the Commissioner will not be presenting his draft budget to the Federal Council until the spring, after the Act has entered into force. We do not yet know which year this will be. The Federal Council will then forward the draft, unchanged, to the Federal Assembly, which will decide by the following winter whether, or by how much, it will increase our budget.

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

2005	22
2010	23
2018	24
2019	24
2020	27

#### Services

The FDPIC's duties as the data protection authority for the federal authorities and the private sector have been divided into four services groups in line with the New Management Model (NPM): consultancy, supervision, information, and legislation. During the reporting year running from 1<sup>st</sup> April 2019 to 31 March 2020, 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	16,5%	
Consultancy - Federal Administration	18,8%	
Collaboration with Cantons	2,5%	
International Cooperation	12%	
<b>Total Consultancy</b>		<b>49,8%</b>
Supervision	16%	
Certification	0,1%	
Data collection register	0,6%	
<b>Total Supervision</b>		<b>16,7%</b>
Information	18,7%	
Education, speeches and presentations	5,5%	
<b>Total Information</b>		<b>24,2%</b>
Legislation	9,3%	
<b>Total Legislation</b>		<b>9,3%</b>
<b>Total Datenschutz</b>		<b>100,0%</b>

## Consultancy

As set out in the opening chapter on ‘Current challenges and priorities’, the FDPIC still faces growing demand to provide consultancy services, since he is required to support large digital projects. Owing to the need to step up our supervisory activity, the proportion of staff working in consultancy has declined by around four percent, to 49,8 percent. In the FDPIC’s inspection plan for 2020, twelve large projects are currently receiving support in the form of consultancy.

Table 6: Consultancy for large-scale projects in 2019

Fundamental rights	1
Traffic and transport	1
Finance	1
Health / Employment	3
Security	2
Telecommunications	1
Media	1
Commerce and economy	2
<b>Total</b>	<b>12</b>

The FDPIC’s resources have not been increased in line with the heightened technological risks of re-identification and misappropriation of data or with the wider challenges digitalisation poses. Therefore, he is not able to provide timely support to the extent required to fully meet the increased demand for project consultancy. Over the course of the reporting period, three teams from the Data Protection Directorate replied to around 65 queries 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 draft complete revision of the FADP also stipulates a wider-ranging obligation for the FDPIC to directly handle individual complaints from Swiss persons.

We have also had to make cuts to other positions in the consultancy group, including those of staff working on international cooperation. Big data and artificial intelligence are becoming a business model in an increasing number of 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 in previous years.

## 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 the 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 and the current reporting period, this proportion has been brought back to around 17 %.

Our inspection plan for 2020 shows that around fifteen comprehensive inspections can be carried out with these resources. Compared with 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.

### Legislation

In the Federal Council's dispatch on the complete revision of the Data Protection Act (Federal Gazette 2017 6943), developments in technology are described as "rapid". This also affects personal data processing by federal government bodies, which is only permissible if specifically authorised in legislation. This entails a large number of new provisions on data processing in federal law, on which the FDPIC has to express his views in various consultation procedures.

This has created a considerable amount of extra work over the last ten years, which in turn has led to a further reduction in the frequency of inspections. Though we managed to halt this trend in the last-but-one reporting period, because of our limited resources we have been forced to limit the justification given for our opinions in consultations and make cuts to services provided in other areas.

### Complete revision of the FADP

As outlined in the last annual report, modern working tools – such as privacy impact assessments – have developed out of experience in the current digital environment. It has therefore become second nature for the FDPIC to use them when supporting large digital projects (see Table 6).

In order to create legal certainty in relation to the use of these tools and the FDPIC's associated supervisory role, it is essential for them to be anchored in both the GDPR and Swiss data protection law, as the ongoing complete revision of the Data Protection Act provides. Since it is still difficult to say when the new FADP will enter into force, our authority must make pragmatic use of the new tools with the existing staff resources.

### Participation in commission consultations and hearings by parliamentary commissions

When the FDJP/FCh subcommittee of the Council of States Control Committee (CC-CS) visited the FDPIC's offices in the previous period, we presented the results of the pilot project 'Acceleration of Dispute Resolution'. In an interview with the subcommittee in April 2019, we had the opportunity to explain to them more about the successful conversion of the pilot project to standard procedure.

In February 2020, an interview was held with the Political Institutions Committee of the Council of States to discuss the systematic use of the OASI number by authorities (amendment of OASIA), and in October 2019 an interview took place with the FDHA/DETEC of the CC-N to discuss the Electronic Patient Records (EPRs). Furthermore, in April and May 2019 we took part in the discussion about the Federal Act on Electronic Means of Identification on the Council of States' Legal Affairs Committee (LAC-C).

### Assessment criteria

Whether and to what extent the FDPIC is allocated additional resources is a matter for the political authorities to decide. Their discretionary judgments 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 the digital society. The FDPIC must be able to act autonomously.

This requires appropriate and sufficient resources in terms of staff, materials, technology and finance. 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 groups (see Table 7):

### Services and resources in the field of freedom of information

Having undertaken a year-long trial in 2017, the Freedom of Information unit, which continues to have 3,6 staff positions, 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 remains high and, in most cases, statutory time limits were only exceeded in cases where the procedures and content were complicated. However, the current reporting year has also shown that when the number of dispute settlement requests increases, numerous requests are submitted within a short time period and vacant positions go unfilled, the unit quickly falls behind and the statutory time limits for completing the dispute resolution procedure cannot be met (see chapter 2.3).

If the upward trend in dispute settlement requests – particularly complex ones – continues, there is a risk that the processing backlog will impact negatively on newly-opened cases.

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 actively influences all special norms and regulations created at national and international level. He helps the parties affected to formulate rules of good practice.

## 3.2 Communication

### **Expansion due to additional tasks and lack of critical mass**

We seek to effectively inform media representatives and the general public about privacy-related issues and the principle of freedom of information in administration, and to engage in relevant dialogue. The website, which attracts around 2000 visitors daily, remains central to communication. In the year under review, the Swiss federal parliament drove forward the discussions about the complete revision of the Data Protection Act (FADP). The likely entry into force of this Act will only increase demand for information from the public, businesses and authorities.

Over the course of this reporting year, the 1,5 FTEs in the Communications department continued to focus on media support for key operational activities. As the revised FADP stipulates new obligations for the business sector and additional duties and powers for the FDPIC, the Media unit will be expanded to 2,5 full-time equivalents, which will also make it easier for people to contact the unit. The job advertisement was published before the end of the reporting period. The primary focus of the role will be communication about the revised Act and taking appropriate information and awareness-raising measures.

These will include cross-media content and audiovisual formats. However, the top priority will be reviewing and updating our existing factsheets, clarifications and guides for consistency with the new provisions of the Act and related ordinance, and creating brand new guidance documents.

### **Extensive media coverage, at home and abroad**

Media interest in data protection continues to intensify. Due to our role in supervising the Libra project, the FDPIC received a larger number of enquiries from foreign media and engaged in more dialogue with international data protection authorities. Media attention was reflected in the many opinions published by the Commissioner and, in particular, an occasionally high profile on TV formats. Some 2000 opinion pieces and articles were published in the print and radio/TV media monitored by the FDPIC, mostly on the subject of data protection but also on the principle of freedom of information in administration. Around 8800 mentions of the Commissioner or the spokespeople were counted while observing the key social media and online platforms. We handled around 450 media enquiries in all.

Members of the public and companies used e-mail, post or the telephone hotline to address their concerns and questions to our experts and we received around 3000 enquiries via these channels.

The Commissioner again attended around forty events as a speaker or panellist. The organisers of these events included associations and clubs, educational establishments, public authorities, and companies, as well as organisations involved in digitalisation. The Commissioner also appeared as a panellist at the third Swiss Digital Day and took the opportunity to raise awareness of protecting privacy in high-circulation corporate magazines in areas such as transport, finance and health.

### Federal and cantonal data protection authorities joined forces for International Data Privacy Day

International Data Privacy Day, an initiative of the European Council, has been held on 28 January each year since 2007. Its aim is to raise public awareness of the protection of privacy, strengthen the right to informational self-determination and bring about a lasting behavioural shift with regard to the use of new technologies.

In January 2020, the FDPIC and the cantonal data protection authorities issued a joint communication about the growing risks to privacy in private and public transport. These risks stem specifically from the use of video to record movements and the creation of movement profiles, which are becoming more commonplace with the advent of ever more sophisticated mobility apps and intelligent vehicles ('connected cars').



## Opinions, recommendations and publications

The Commissioner published a range of opinions and statements on current projects and events during the year under review, on subjects including the following:

- The Geneva-based Libra Association which, in July 2019, announced the launch of a project for a global cryptocurrency.
- US application Clearview which, as transpired in January 2020, gathers and commercialises huge amounts of facial data from public sources.
- Facebook's election feature, which was used in Switzerland during the Federal elections in October 2019.
- The implications of Brexit for Switzerland's international data traffic from 31 January 2020 onwards.
- Postfinance's unequal treatment of Swiss nationals compared with EU nationals when using Voiceprint in the customer center
- On various aspects, which generated a great deal of interest in connection with the Corona crisis, such as the Proximity Tracing App, the FOPH's access to Swisscom location data or the use of video chats

On the FDPIC's website we published 23 recommendations on the principle of freedom of information.

The interactive Think Data platform, which is linked on our website, enabled us to raise broader public awareness of greater data protection and transparency. Privacy recommendations are made on the platform based on specific scenarios. Think Data is a project by an interdisciplinary working party (Thinkservices) which the FDPIC helped to set up and continues to support.

As in the previous year, the annual activity report is being published in four languages, and is available both in printed form and as an ePaper linked on the website

## Website still the key channel for our communication

The website is the FDPIC's central communication channel. We attract around half a million visitors each year, or 2000 on a single working day. Two out of five visitors are from abroad, mostly from the European states but also from overseas or Asia. Content is usually available in three languages, German, French and Italian. We also publish content that is relevant to foreign users in English. We are gradually optimising our website.

We also communicate via Twitter at @derBeauftragte. The aim is to make it easier for our followers and a wider community interested in data protection to quickly access relevant information. Due to limited resources and a number of other reasons, we have decided against the official use of other social media platforms.

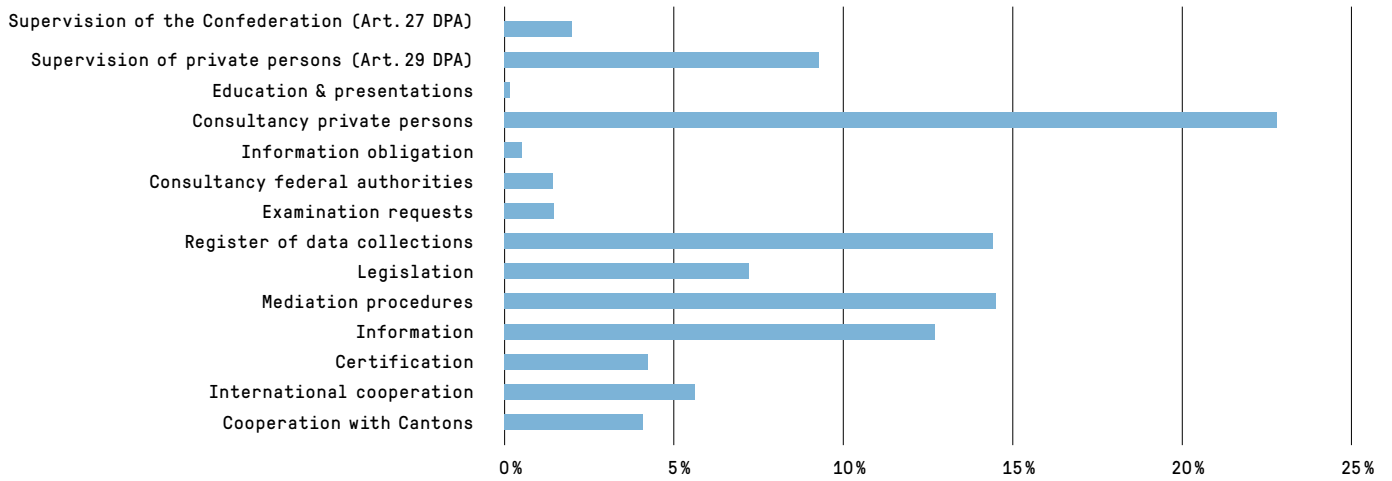




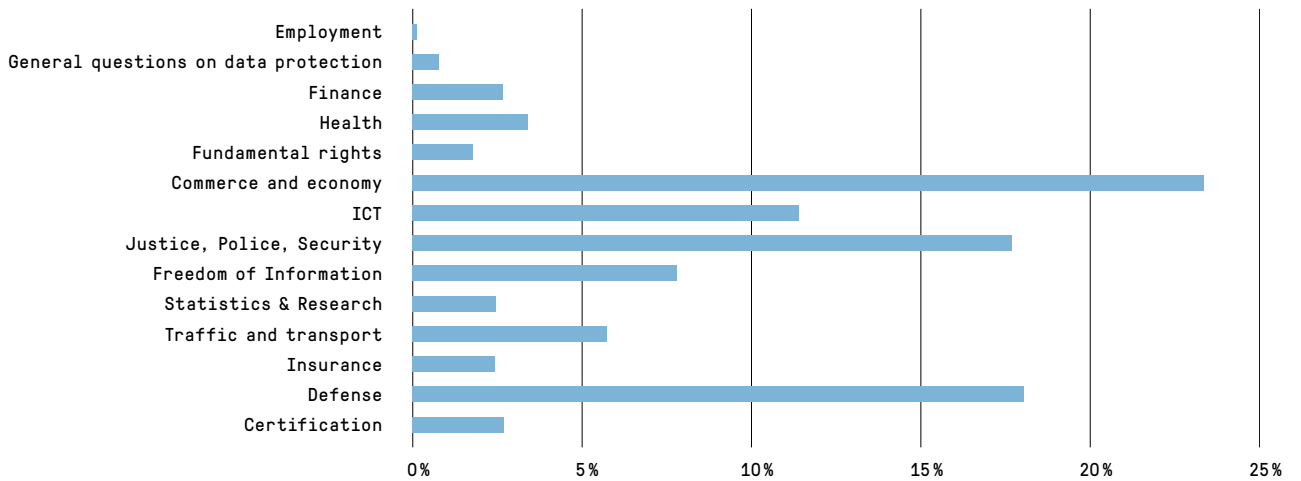
### 3.3 Statistics

#### Statistics on FDPIC's activities from 1<sup>st</sup> April 2018 to 31 March 2019 (Data protection)

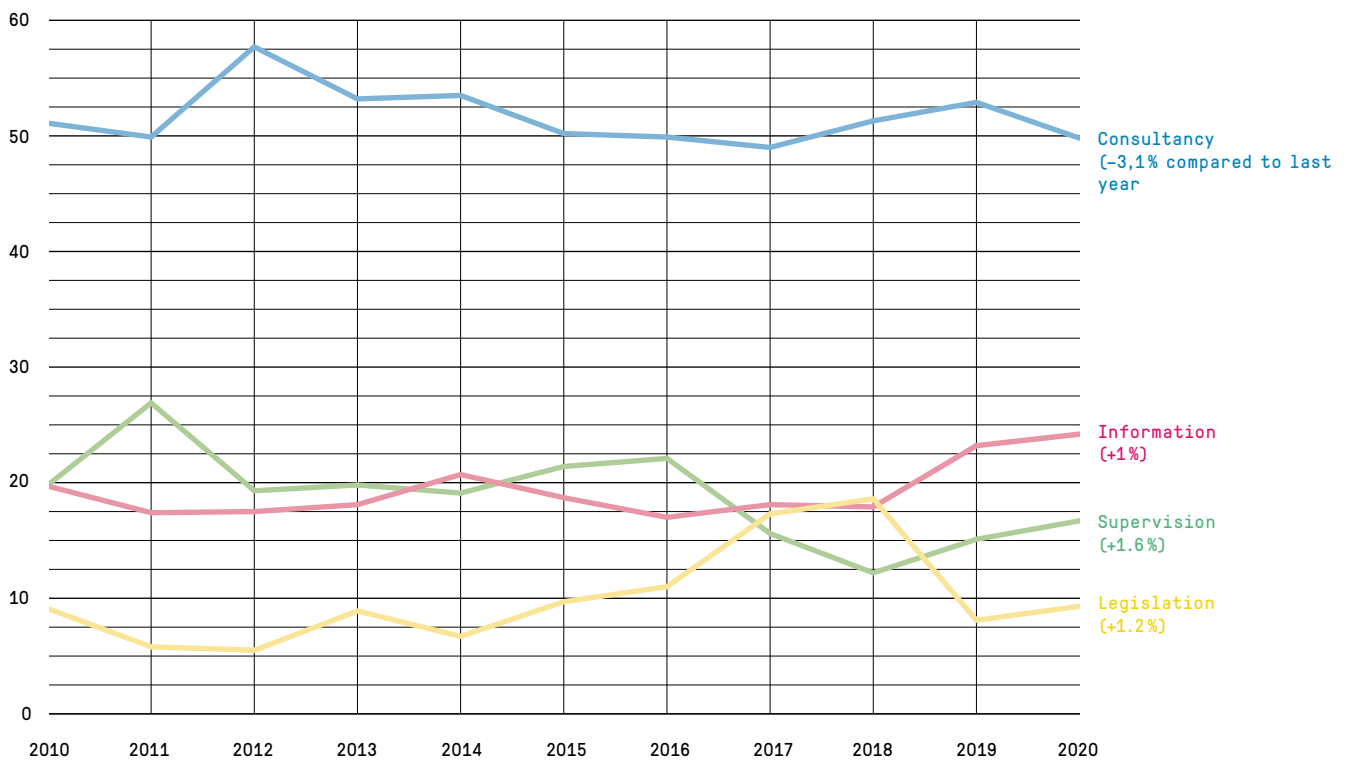
##### Workload per tasks



##### Workload per material



**Multi-year comparison**  
(as a percentage)



## Overview of applications from 1<sup>st</sup> January to 31 December 2019

Department	Number of requests	Access completely granted	Access completely denied	Access Partially granted/suspended	Request withdrawn	Pending requests	No document available
FCh	24	12	3	2	4	0	3
FDFA	168	89	15	38	7	10	9
FDHA	126	52	15	31	8	9	11
FDJP	48	27	8	9	2	1	1
DDPS	225	193	6	14	6	4	2
FDF	102	49	17	25	2	4	5
EAER	100	50	11	27	3	7	2
DETEC	112	67	9	25	3	7	1
OAG	10	3	1	0	3	1	2
PS	1	0	1	0	0	0	0
<b>Total 2019 (%)</b>	<b>916 (100)</b>	<b>542 (59)</b>	<b>86 (9)</b>	<b>171 (19)</b>	<b>38 (4)</b>	<b>43 (5)</b>	<b>36 (4)</b>
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)	-
Total 2010 (%)	239 (100)	106 (44)	62 (26)	63 (26)	0 (0)	8 (3)	-

## Statistics on applications for access under the Freedom of Information Act from 1<sup>st</sup> January to 31 December 2019

	Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
Federal Chancellery FCh	BK	14	6	3	2	1	0	2
	EDÖB	10	6	0	0	3	0	1
	<b>Total</b>	<b>24</b>	<b>12</b>	<b>3</b>	<b>2</b>	<b>4</b>	<b>0</b>	<b>3</b>
Federal Department of Foreign Affairs FDFA	EDA	168	89	15	38	7	10	9
	<b>Total</b>	<b>168</b>	<b>89</b>	<b>15</b>	<b>38</b>	<b>7</b>	<b>10</b>	<b>9</b>
Federal Department of Home Affairs FDHA	GS EDI	8	3	2	3	0	0	0
	EBG	3	2	0	0	0	0	1
	BAK	4	3	0	1	0	0	0
	BAR	2	2	0	0	0	0	0
	METEO CH	1	1	0	0	0	0	0
	NB	0	0	0	0	0	0	0
	BAG	35	6	3	14	3	2	7
	BFS	6	3	3	0	0	0	0
	BSV	15	12	0	0	0	3	0
	BLV	14	3	1	7	0	0	3
	SNM	0	0	0	0	0	0	0
	SWISS MEDIC	31	14	3	5	5	4	0
	SUVA	7	3	3	1	0	0	0
	<b>Total</b>	<b>126</b>	<b>52</b>	<b>15</b>	<b>31</b>	<b>8</b>	<b>9</b>	<b>11</b>
Federal Department of Finance FDF	GS EJPD	6	5	0	1	0	0	0
	BJ	12	8	0	4	0	0	0
	FEDPOL	5	2	0	3	0	0	0
	METAS	4	3	1	0	0	0	0
	SEM	9	3	3	0	1	1	1
	Dienst ÜPF	2	0	2	0	0	0	0
	SIR	4	2	0	1	1	0	0
	IGE	0	0	0	0	0	0	0
	ESBK	3	3	0	0	0	0	0
	ESchK	0	0	0	0	0	0	0
	RAB	2	0	2	0	0	0	0
	ISC	1	1	0	0	0	0	0
	NKVF	0	0	0	0	0	0	0
	<b>Total</b>	<b>48</b>	<b>27</b>	<b>8</b>	<b>9</b>	<b>2</b>	<b>1</b>	<b>1</b>

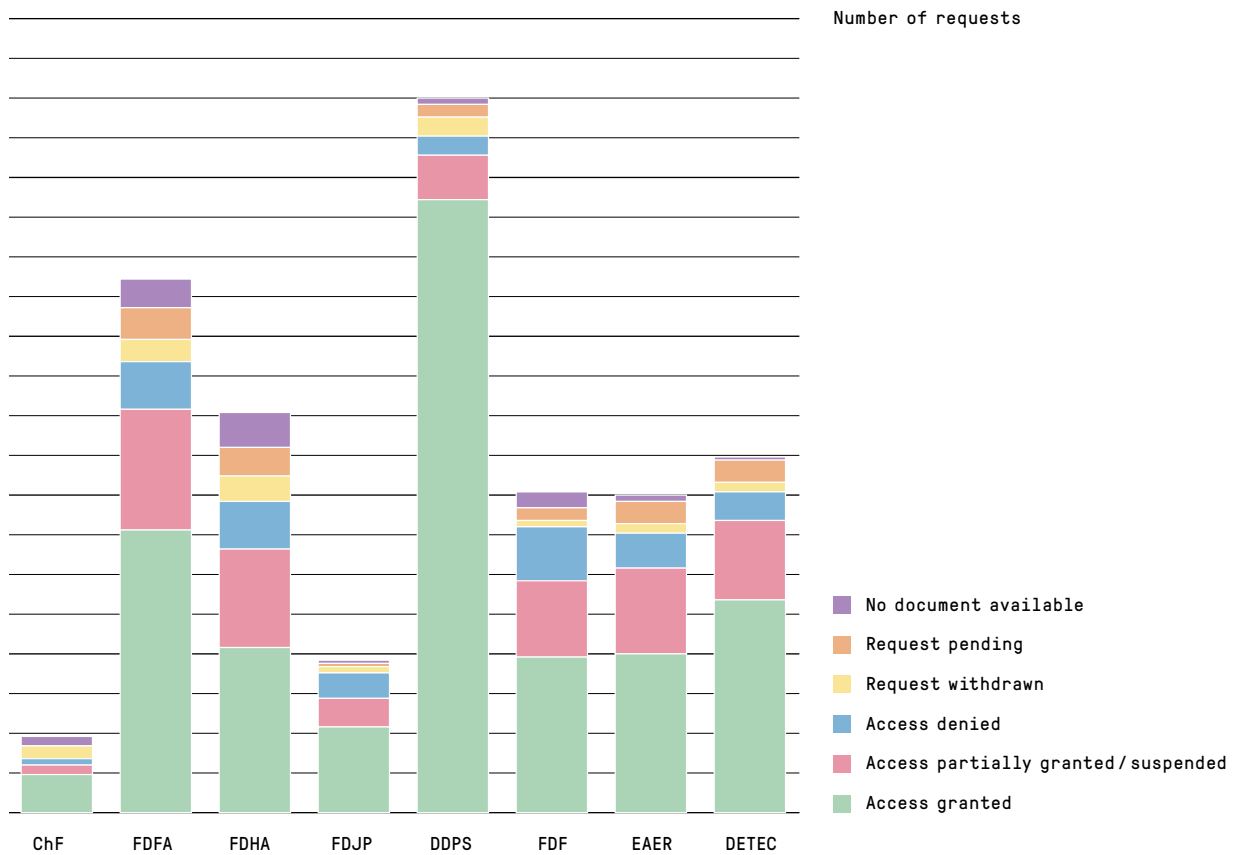
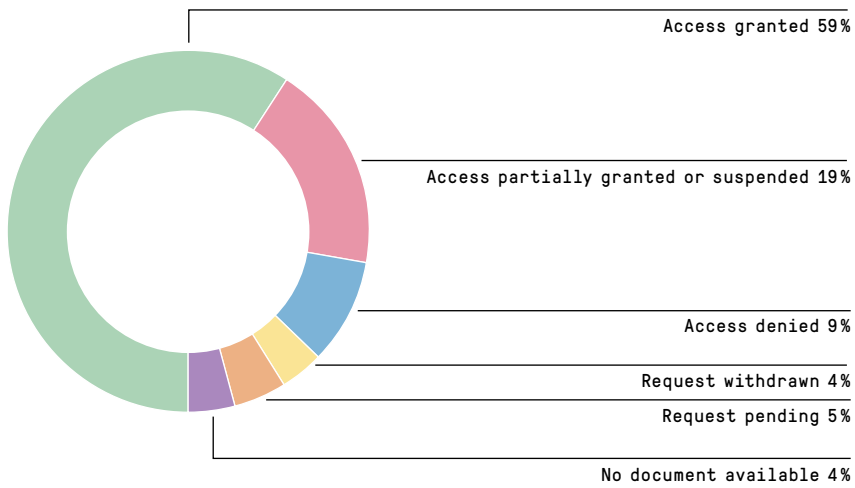
Department/ Office	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available	
<b>Federal Department of Defence, Civil Protection and Sport DDPS</b>	GS DDPS	5	4	0	1	0	0	
	Defence/ Army	24	9	1	9	3	1	
	FIS	10	1	3	3	1	1	
	armasuisse	7	4	1	1	0	1	
	FOSPO	175	172	1	0	1	1	
	FOCP	2	2	0	0	0	0	
	swisstopo	2	1	0	0	1	0	
	OA	0	0	0	0	0	0	
	<b>Total</b>	<b>225</b>	<b>193</b>	<b>6</b>	<b>14</b>	<b>6</b>	<b>4</b>	<b>2</b>
<b>Federal Department of Finance FDF</b>	GS FDF	16	4	7	3	0	2	
	FITSU	4	1	2	1	0	0	
	FFA	6	4	0	2	0	0	
	FOPER	3	3	0	0	0	0	
	FTA	14	8	3	2	0	0	
	FCA	16	5	3	6	2	0	
	FOBL	4	4	0	0	0	0	
	FOITT	5	5	0	0	0	0	
	SFAO	10	6	1	1	0	1	
	SIF	4	2	1	1	0	0	
	PUBLICA	0	0	0	0	0	0	
	CCO	20	7	0	9	0	1	
	<b>Total</b>	<b>102</b>	<b>49</b>	<b>17</b>	<b>25</b>	<b>2</b>	<b>4</b>	<b>5</b>
	<b>Federal Department of Economic Affairs, Education and Research EAER</b>	GS EAER	10	4	1	4	0	1
SECO		34	14	7	11	1	1	
SERI		3	2	0	0	0	0	
FOAG		14	5	2	2	1	3	
FONES		1	0	0	1	0	0	
FHO		0	0	0	0	0	0	
PUE		4	1	1	1	0	1	
COMCO		15	12	0	3	0	0	
ZIVI		1	1	0	0	0	0	
FCAB		2	2	0	0	0	0	
SNSF		1	0	0	1	0	0	
SFIVET		0	0	0	0	0	0	
ETH Board		9	7	0	1	0	1	
Innosuisse		6	2	0	3	1	0	
<b>Total</b>		<b>100</b>	<b>50</b>	<b>11</b>	<b>27</b>	<b>3</b>	<b>7</b>	<b>2</b>

	Department/ Office	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Request pending	No document available
<b>Federal Department of the Environment, Transport, Energy and Communications DETEC</b>	GS DETEC	10	8	1	0	0	1	0
	FOT	11	8	0	3	0	0	0
	FOCA	15	7	2	2	0	3	1
	SFOE	12	6	0	4	1	1	0
	FEDRO	10	9	0	0	0	1	0
	OFCOM	4	3	0	0	0	1	0
	FOEN	35	19	3	12	1	0	0
	ARE	0	0	0	0	0	0	0
	ComCom	1	1	0	0	0	0	0
	ENSI	10	3	2	4	1	0	0
	PostCom	1	1	0	0	0	0	0
	ICA	3	2	1	0	0	0	0
	<b>Total</b>	<b>112</b>	<b>67</b>	<b>9</b>	<b>25</b>	<b>3</b>	<b>7</b>	<b>1</b>
	<b>Office of the Attorney General OAG</b>	OAG	10	3	1	0	3	1
<b>Total</b>		<b>10</b>	<b>3</b>	<b>1</b>	<b>0</b>	<b>3</b>	<b>1</b>	<b>2</b>
<b>Parliamentary Services PS</b>	PS	1	0	1	0	0	0	0
	<b>Total</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>

### Number of requests for mediation per category of applicants

Category of Applicant	2019
Media	34
Privat Persons (or not exact assignment possible)	40
Interested parties (associations, organisations, companies, etc.)	7
Lawyers	5
Companies	47
<b>Total</b>	<b>133</b>

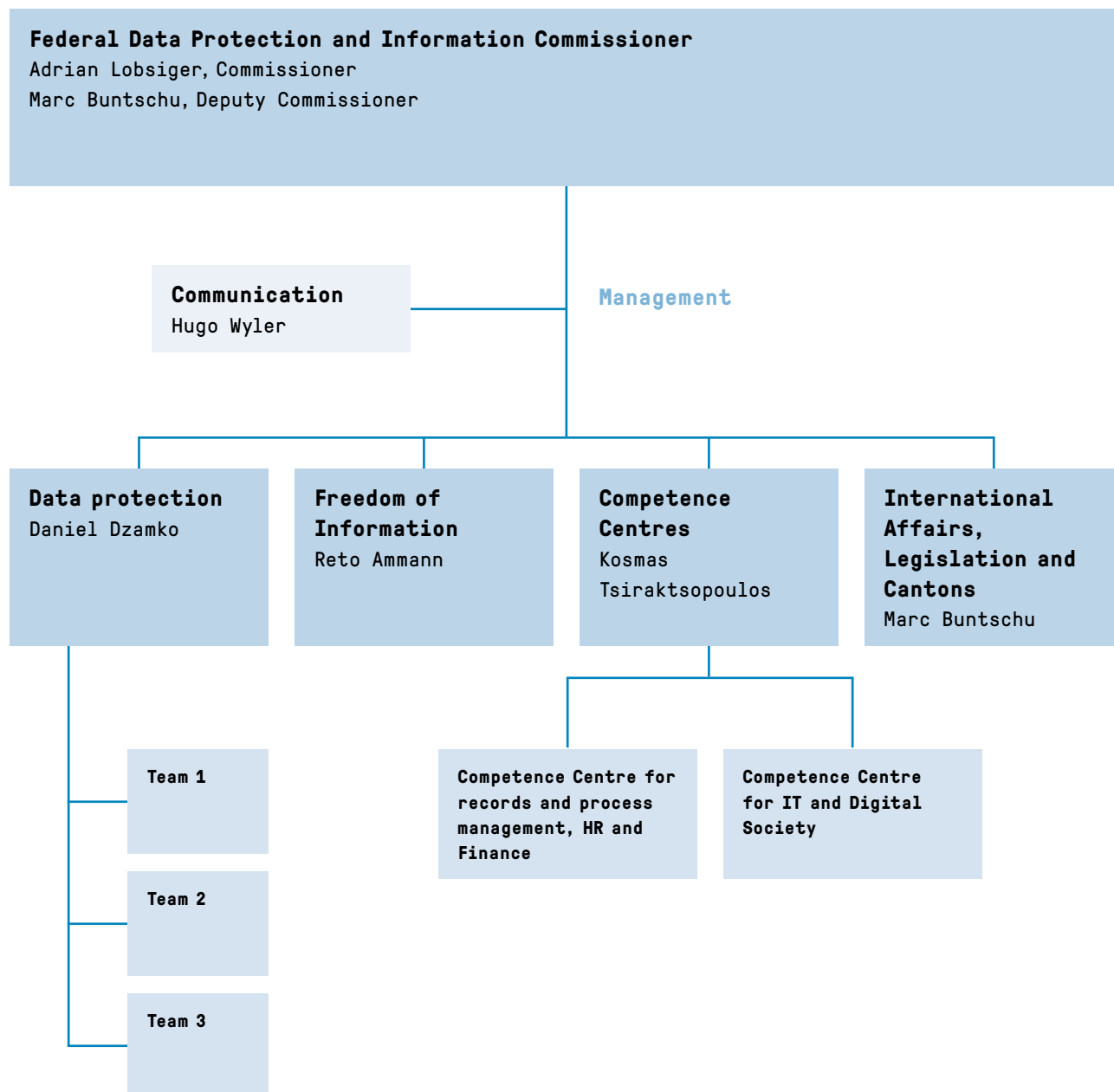
**Applications for access in the federal administration  
from 1<sup>st</sup> January to 31 December 2019**





### 3.4 Organisation EDÖB (Status 31 March 2020)

#### Organisation chart



## Employees of the FDP

Number of employees	37		
FTE	30,8		
per gender	Women	19	51%
	Men	18	49%
by employment level	1-89%	25	68%
	90-100%	12	32%
by language	German	29	78%
	French	7	19%
	Italian	1	3%
by age	20-49 years	22	59%
	50-65 years	15	41%
Management	Women	3	33%
	Men	6	67%



## Abbreviations

<b>ADR</b> Alternative Dispute Resolution body	<b>FADP</b> Federal Act on Data Protection	<b>SDPA</b> Schengen Data Protection Act
<b>AEOI</b> Automatic exchange of information	<b>fedpol</b> Federal Office of police	<b>Seco</b> State Secretariat for Economy
<b>AFAPDP</b> Association of French speaking data protection authorities	<b>FEDRO</b> Federal Roads Office	<b>SEM</b> State Secretariat for Migration
<b>CbCRA</b> Exchange of Country-by-Country Reports from Multinational Enterprises	<b>FoIA</b> Freedom of Information Act	<b>SIF</b> State Secretariat for International Finance
<b>CJEU</b> Court of Justice of the EU	<b>FoIO</b> Ordinance on Freedom of Information in the Administration	<b>SIRENE</b> Supplementary Information Request at the National Entry
<b>CNIL</b> French data protection authority	<b>FTC</b> Federal Trade Commission of the US	<b>SIS II</b> Schengen Information System (2 <sup>nd</sup> generation)
<b>Convention 108+</b> Modernised Data Protection Convention of the Council of Europe	<b>GDPR</b> General Data Protection Regulation of the EU	<b>T-PD</b> Consultative Committee on Convention 108
<b>DoC</b> US Department of Commerce	<b>ICO</b> Information Commissioner's Office (Data protection authority of the UK)	<b>VIS</b> Visa Information System
<b>EDPB</b> European Data Protection Board	<b>OECD</b> Organisation for Economic Cooperation and Development	
<b>E-ID Act</b> Federal Act on Recognised Electronic Means of Identification	<b>PCLOB</b> Privacy and Civil Liberties Oversight Board	
<b>EIDCOM</b> Commission to supervise and control applicants of the E-ID	<b>PIC</b> Political Institutions Committee	
<b>EPR</b> Elektronik Patient Record	<b>PNR</b> Passenger Name Record	
<b>Eurodac</b> EU fingerprint database for identifying asylum seekers	<b>Privatim</b> Conferende of the cantonal data protection commissioners	
	<b>RIPOL</b> Computerised police research system	

## Figures and tables

### Figures

Figure 1: Evaluation of requests for access – trend since 2006 .....S. 65

Figure 2: Fees charged since the FoIA entered into force..... S. 66

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

### Tables

Table 1: Processing time of mediation procedures ..... S. 69

Table 2: Amicable outcomes.....S. 70

Table 3: Pending mediation procedures .....S. 70

Table 4: Number of employees for FADP concerns ..... S. 80

Table 5: Services in data protection... S. 80

Table 6: Consultancy for large-scale projects in 2019 ..... S. 81

Table 7: Outcome objectives FDPIC..... S. 83

The pictures in this report are conceived as a series of photographs detached from the content and convey our everyday mobility world, which also raises numerous data protection issues. Individual parts of the photographs are shown in pixelated form to draw attention to the problem of identification and at the same time make people and companies unidentifiable. The pictures were taken by photographer Ben Zurbriggen from Biel.

## 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](http://www.bundespublikationen.admin.ch)

Art.-Nr. 410.027.ENG

Layout: Duplex Design GmbH, Basel

Photography: Ben Zurbriggen

Characters: Pressura, Documenta

Print: Ast & Fischer AG, Wabern

Paper: PlanoArt®, woodfree bright white



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

E-Mail: [info@edoeb.admin.ch](mailto:info@edoeb.admin.ch)

Website: [www.derbeauftragte.ch](http://www.derbeauftragte.ch)

 [@derBeauftragte](https://twitter.com/derBeauftragte)

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

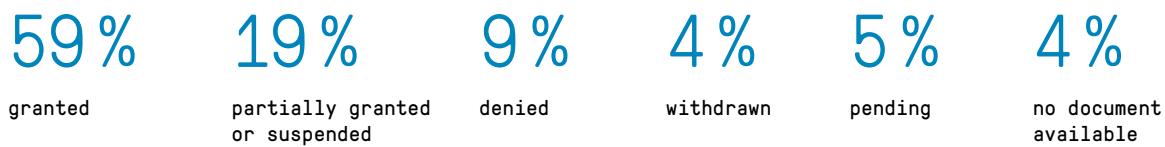
Fax: +41 (0)58 465 99 96

## Key figures

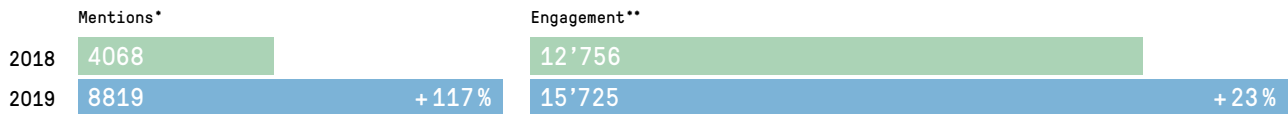
### Workload data protection



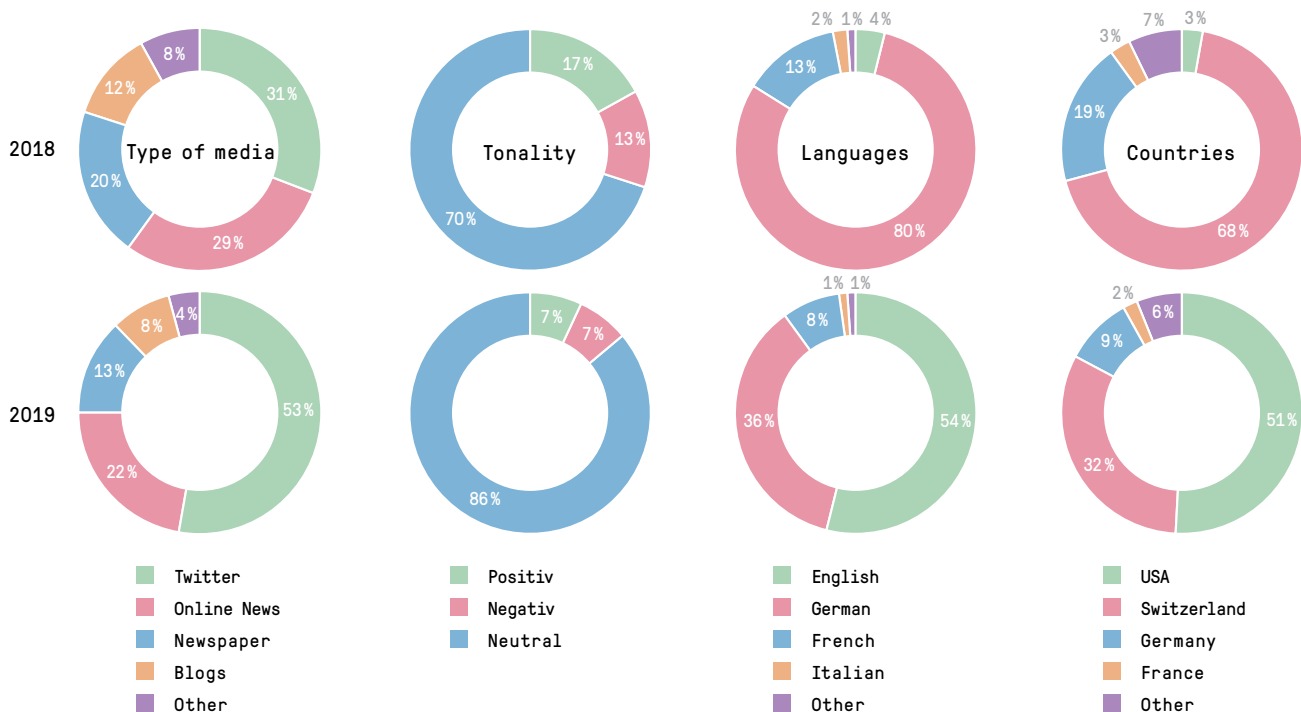
### Applications for access Freedom of Information (FoIA)



### 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.)



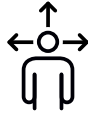


## Data protection concerns



### 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.



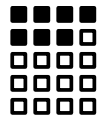
### Risk analysis

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



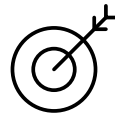
### Data correctness

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.