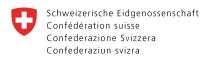
26th Annual Report 2018/19Federal Data Protection and Information Commissioner



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

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

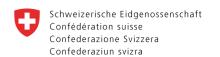
y @derBeauftragte

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

Fax: +41 (0)58 465 99 96

Annual	Report 2018/2019	
of the	Federal Data Protecti	.on
and Int	formation Commissioner	1

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 2018 and 31 March 2019.





Foreword

Switzerland holds a top spot in digital competitiveness according to the World Economic Forum and World Competitiveness Center's rankings. To ensure we retain this position, the Federal Council develops strategies and action plans to promote the digitalisation of the economy and state authorities.

Data protection can also benefit Switzerland's attractiveness as a hub for innovation, since technological developments, which protect people's privacy and give them control over their digital lives, improve a country's attractiveness.

In the race for innovation, we should not forget to protect Switzerland's existing advantages as a business and research venue. In 1992 – almost thirty years ago – the Swiss legislator had the foresight to introduce an internationally recognised Data Protection Act, which to this day lets Swiss businesses exchange data with companies from important trading nations without further legal restrictions and requirements. And, as we know, data are in great demand.

Digitalisation has a profound impact on the privacy of around four billion internet users worldwide. From these considerations, the EU and the EEA member states increased the data protection level to safeguard their residents. In May 2018, new uniform, modern regulations took effect, to continue exchange data across borders without hindrance. This cross border data exchange also includes Japanese and within the restricted framework of the Swiss-U.S. Privacy Shield certified US companies.

Switzerland is widely expected to continue to participate in the free data exchange, given its ambitions as an education, technology and business hub. In September 2017, the Federal Council presented a complete revision of the Federal Act on Data Protection with an accompanying report to the Federal Parliament, thus triggering the legislative process through its two chambers. It is therefore up to Parliament, where the draft act is currently pending, to bring data protection for Swiss residents up to a standard comparable to that of our European neighbour countries. When this process is completed and our residents are more appropriately protected, the access of businesses to free data sharing will be ensured and Switzerland's reputation as a digital nation will once again be preserved.

Adrian Lobsiger

Federal Data Protection and Information Commissioner



Current challenges 8

1.1 Digitalisation and fundmental rights 18	1.5 Health4
 Revision of the Federal Data Protection Act (FADP) Data protection guidelines in the context of 	 Statistics project using insurers' individual datasets (BAGSAN)
elections and votes	- Electronic patient record gives rise to new tasks
 Systematic use of the OASI number by the authorities Parameters for a Swiss data policy 	 "Helsana+" bonus programme on trial: the FDPIC calls upon the Federal Administrative Court
- Data linkage for statistical purposes	 Risks inherent in the rapid proliferation of "personalised health" data
Focus I	4.c Employment
Electronic proof of identity (E-ID)	1.6 Employment
The "SwissID"	Online application procedures and interviews: the key aspects to consider
1.2 Justice, Police, Security 26 - Police counterterrorism measures	- Combating illegal employment in the canton of Valais
- Certain improvements to the Swiss-U.S. Privacy	1.7 Insurance4
Shield required	 New observation article for social insurance
 Release of airline passenger data in EU states 'Swiss' booking system – Calls for measures to prevent data misuse 	 SUVA: more transparency in research using insured persons' data
Focus II	1.8 Traffic5
Schengen Data Protection Act now in force	 Multimodal mobility – Safeguards of informational self-determination are essential
Schengen evaluation of Switzerland sufficient resources required	- Privacy compliance of new public transport apps
- Automated vehicle searches and traffic surveillance	1.9 International5
1.3 Taxation and finance	 Supervision Coordination Groups on the SIS II, VIS and Eurodac information systems
 Release of personal data to foreign tax authorities Objection against FDF in the FTA case still pending 	 Sub-Working Group on "Border, Travel & Law Enforcement"
Recommendation against Zentralstelle für Kreditinformation (ZEK)	 Swiss Data Protection Authorities Coordination Group for the Implementation of the Schengen Association Agreement
1.4 Commerce and economy	 International Conference of Data Protection and Privacy Commissioners
 Data theft case at Swisscom concluded without formal action being taken 	 Conference of European Data Protection Authorities
Data theft at EOS – storage of unnecessary patient data	 OECD Working Party on Security and Privacy in the Digital Economy (SPDE)
- Use of ricardo.ch data within the Tamedia group	- The Francophone Association of Data Protection
 Case investigation at smart-TV manufacturer concluded 	Authorities (AFAPDP) Focus III
- Sporting goods retailer Decathlon - better	The GDPR – also applicable in Switzerland in some instances
information needed when gathering data	Council of Europe – Switzerland should ratify the adapted

Freedom of Information

2.1 Generally	64
2.2 Requests for access - Constant growth	65
2.3 Mediation procedure	. 68
Proportion of amicable outcomesNumber of pending cases	
2.4 Office consultations and other commentaries	. 70
 Complete revision of the Federal Act on Public Procurement 	
 Office consultation on the approval of tariff structures in health insurance 	

The FDPIC

3.1 Duties and Resources74
- Services and resources in the field of data protection
- Services and resources in the field
of freedom of information
3.2 Communication
 Lots of awareness-raising and extensive media coverage
 Federal and cantonal data protection authorities joined forces for International Data Privacy Day
 Various guidance documents and recommendations published
- Website still primary channel for our communication
3.3 Statistics 80
 Statistics on FDPIC's activities from 1 April 2018 to 31 March 2019 (Data protection)
 Statistics on applications for access under the Freedom of Information Act from 1 January to 31 December 2018
 Overview of applications for access per Department and the Federal Chancellery
 Number of requests for mediation
 Overview applications for access in the federal administration
3.4 Organisation
Abbreviations 88
Figures89
Impressum
In the cover
Key figures
Data protection concerns

Current challenges

Current challenges

I Digitalisation

Personal data processing is continuously shaped by the dynamic development of the information and telecommunications technology in a globally interlinked economy. This has a major impact on work, leisure and the purchasing habits of the Swiss population.

Technologie und Wirtschaft

The technological and economic potential for attacks on people's privacy and rights to control their digital lives remains a great threat. The Federal Data Protection and Information Commissioner (FDPIC) attributes this primarily to two developments:

• In the internet age, business models can potentially target around four billion users worldwide. Silicon Valley tech firms such as Google, Amazon and Facebook dominate markets, and a type of 'free' model has become the standard for providing internet-based communication and information services. Instead of charging for their online services, the providers require data from their customers. The providers then process these data using algorithms and specific analysis methods in order to send the customer targeted advertising. The provider then auctions the advertising space to the third party, which offers the highest price. A few providers are so successful in pursuing this business model that they attract billions of customers to their 'free' services. They can feed their algorithms streams of customer data to let them upscale the analysis of user behaviour and make an astronomical turnover on online advertising markets - while targeted advertising and political messaging

pose a growing risk to users. Meanwhile, newspapers, radio and television are facing a decline in advertising income.

Telecommunications companies in

Switzerland recently announced that they will equip network infrastructure for fifth generation bandwidths (5G), meaning that 5G technology will soon be part of our lives and the capacity and speed of mobile data flows will once again increase significantly. The previous report discussed the rapidly growing number of sensors which record human images and voices, both in private and public spaces, and feed this information to artificial intelligence. This trend is only set to accelerate.

Society and data politics

This reporting year has seen further growth in public criticism of the companies behind social networks and search engines, which pursue a business model of collecting data in return for providing 'free' services worldwide.

Given the growing volume of customer data gathered and the increasing complexity and autonomy of the analysis technologies, it is increasingly difficult for the providers under criticism to guarantee a sufficient standard of data protection. Not only do they have to provide their customers with easily understandable and complete information about the processing of customer data, but they also have to give them sufficient opportunity to freely accept or reject all aspects of this data processing. To fulfil this duty, they are required to invest in data protection-friendly applications which give customers the information they require and allow them to make choices in just a few clicks. Digital products must let users protect their privacy and give them the freedom to run their own digital lives. These requirements must already be taken into account during the development of digital applications. Providers who pay regulatory lip service to these requirements and solve issues of protection mechanically risk losing their customers' trust and will at some point attract the attention of the FDPIC.

Providers who pay regulatory lip service to these requirements and solve issues of protection mechanically risk losing their customers' trust and will at some point attract the attention of the FDPIC.

In the reporting year, the data protection authorities of the EU and EEA member states started to impose large fines on companies which fail to ensure transparency and customer control, as provided for by the General Data Protection Regulation (GDPR). According to preliminary information available to the FDPIC, Swiss companies which process data on EU residents have also been affected by the proceedings of data protection authorities in the EU. Competition authorities are also increasingly involved in data protection. In this reporting period, the German Federal Cartel Office required Facebook to make acceptance of its terms and conditions

of use separate from other services it

provides, justifying this on the basis of

Facebook's dominant market position. It remains to be seen whether the platforms which dominate the market will continue to offer 'free services', given pressure from regulatory authorities and public criticism. A feasible alternative from the point of view of data protection would be to pursue business models which exclude paying customers from data analysis used to build profiles and from personalised advertising. Paying services of this kind could be run either using decentralised crypto-currencies or via the banking system. They are already widespread in China, for example, because Chinese platform operators charge commission for concluding contracts online.

Legislation

In Switzerland, we are still waiting for Political Institutions Committee of the National Council, which is acting as the first legislative chamber in this case, to finish discussing the complete revision of the Data Protection Act presented by the Federal Council in September 2017. On 12 January 2018, the committee decided to divide the draft into two parts for a complete revision, and the committee dealt firstly with the amendments required for taking on the 'Schengen Acquis'. Then Parliament passed a new Federal Act on the implementation of Directive (EU) 2016/680. This special act, which only applies to data processing by the federal prosecution authorities, came into force on 1 March 2019. The act is not intended to remain in force following the commencement of the completecy revised Data Protection Act, for which there is currently no date. The special act has given FDPIC additional duties and powers regarding the particularly sensitive task of processing police-related personal data, meaning that he will have to prioritise monitoring of the Federal Office of Police(fedpol). At the time of printing this report, it was not yet known whether the Federal Council will provide the additional resources required to do this.

The FDPIC takes part in the National Council's Political Institutions Committee's discussions on the Data Protection Act at the committee's invitation. In these discussions, he has consistently called for a prompt improvement in data protection for Swiss residents and a prompt conclusion of the parliamentary discussions to enable this. However, it is still difficult to predict when the discussions will be concluded.

Though certain business circles may think that the Data Protection Act, which dates back to 1992, and the weak powers it grant the FDPIC are sufficient, the FDPIC's contact with both large and small businesses operating internationally has revealed a keen willingness to invest in credible company data protection. These companies are directly affected by the complete revision and want to offer their Swiss customers protection in line with the new European standards. They also know that, in today's digital world, it is not possible to control risk in projects involving data processing or to keep the public informed without using modern instruments such as privacy impact assessments. The longer Switzerland does not explicitly require the use of such instruments in legislation, the longer companies located here - despite their actual investment in data protection - will face critical questions about the regulatory standard of protection in the country where they are based.

And until this happens, their small, medium-sized and large rivals from EU and EEA member states will make use of this competitive advantage.

Current challenges

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. He therefore requires that providers of digital applications minimise privacy risks at the planning and project stage, document them and submit this documentation to the company and 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 to reduce his own workload, the FDPIC 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 FDPIC also encourages companies to set up their own data protection bodies. However, the cost of consultancy services for private projects continued to grow as a proportion of our complete expenditure over the reporting year (see Chapter 3.1 in this report).

Whereas expenditure on supervisory duties declined significantly in the previous period, it has since climbed back to the 2016/2017 level. However, expenditure is still below the longterm average for previous periods. Since the FDPIC has been continuously under-resourced, this increase required cuts to other services. Moreover, in this reporting period, the FDPIC has not been able to meet justified public expectations sufficiently with regard to its supervision of personal data processing via consumer apps and social networks (see Chapter 3.1 in this report).

The FDPIC has prioritised providing consultancy services for the federal parliamentary elections in autumn 2019: in collaboration with cantonal data protection authorities, he has published a guide on the application of data protection law to personal data processing in the context of elections and popular votes (www.edoeb.admin. ch/voting). This guide reminds all parties involved that personal data on political views and ideology require a much higher standard of protection than data processed for commercial purposes. Political parties are called upon to guarantee exemplary data protection given political parties' central role in the autumn 2019 parliamentary election. When political parties or associated third parties contact voters, they have the right to know what databases and other digital processing methods and technologies were used to identify them.

The longer Switzerland does not explicitly require the use of such instruments in legislation, the longer companies located here – despite their actual investment in data protection – will face critical questions about the regulatory standard of protection in the country where they are based.

III National and international cooperation

The FDPIC has continued to cooperate ever more closely with cantonal and communal data protection agencies, which face the same trends and technologies in personal data processing. For example: the Schengen evaluation (see Chapter 1.2), the election guidelines (see Chapter 1.1) and the joint organisation of the International Data Protection Day.

New European Data Protection Legislation

The GDPR, which came into force on 25 May 2018, also applies to data processing by Swiss companies under certain circumstances. In autumn 2017, the FDPIC published a short report which looks in particular at the extraterritorial validity of the new EU legislation and is regularly updated (www.derbeauftragte.ch, GDPR). We will continue to do everything in our power to advise and support the relevant Swiss companies in applying the GDPR, while also developing a noticeable presence abroad as a regulatory authority.

The continuing transition phase leading up to the commencement of the completely revised Data Protection Act (see Chapters 1.1 and 3.1 in this report) remains challenging for the FDPIC. While data protection authorities in the EU and EEA member states have now received additional staff and make use of their powers to issue rulings and sanctions (see above), the only power the FDPIC has over businesses and most of the Federal Administration at present is the right to make recommendations provided for in the 1992 Data Protection Act. Its resources have also remained largely the same

since 2005. An additional challenge is that the European Commission has started to evaluate the level of data protection in Switzerland.

Following the enactment of the GDPR, the former 'Article 29' group of EU data protection authorities has now become the European Data Protection Board (EDPB). Its primary task is ensuring the uniform application of GDPR. The FDPIC asked for permission to attend meetings permanently as an observer, but this request was turned down. We will take part in plenary sessions only, provided that points concerning the Schengen acquis are discussed.

Evaluation of data protection level

The European Commission is investigating the level of data protection in third countries and last stated that it considers the level of data protection in Switzerland appropriated in 2000. Companies in the EU can therefore exchange personal data with companies in Switzerland without taking further measures. The European Commission is currently re-evaluating whether the level of data protection in Switzerland is appropriate according to the criteria listed in the GDPR. It has announced that it will publish a report setting out its decision on this issue in May 2020. Swiss participation in the evaluation is being coordinated by the Federal Office of Justice and the FDPIC is providing support by making the requested information available (see Chapter 1.9).

Current challenges Current challenges

It would benefit Switzerland if the ongoing evaluation were based not on the 1992 version of the Data Protection Act, but on the completely revised version of the law. However, deliberations on the complete revision by the National Council, which is acting as the first legislative chamber, have not yet been completed (see Chapter I). It would also be beneficial for the Federal Council to sign the modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe, which has been ready for signature since October 2018. The European Commission has repeatedly stated that the ratification of this modernised convention will be a crucial factor in the decision on the appropriateness of the level of data protection in Switzerland.

14

Swiss-U.S. Privacy Shield

In autumn 2018, we carried out a supervisory review of the Swiss-U.S. Privacy Shield as part of a delegation led by the State Secretariat for Economic Affairs. This followed on from the second review of the EU-US Privacy Shield in Brussels. Although weaknesses were identified in the review, the overall functioning of the Privacy Shield has improved since it came into effect.

When political parties or associated third parties contact voters, they have the right to know what databases and other

IV Efficiency measures

In light of the challenges outlined above, the FDPIC reaffirms his strategic aim: to fulfil his statutory duties competently, autonomously and proactively in the new digital world.

FDPIC organisation and management

The reorganisation implemented on 1 April 2017 has been worthwhile, and a consolidation programme (EFFET) building on this reorganisation and on a staff survey was launched during this reporting year. The programme aims to optimise internal collaboration and, by extension, the effectiveness of the FDPIC.

In this reporting year, there have been numerous changes in staff at management level. After 38 years as a data protection expert in the federal government, including 25 years as deputy to the Commissioner, Jean-Philippe Walter retired at the end of 2018. Marc Buntschu, also a French speaker, took Walter's place as Deputy Commissioner and head of International Affairs, Legislation, Cantons. In his former role as head of Data Protection, Buntschu was supersedet on 1 February 2019 by Daniel Dzamko, previously a manager in the Bern cantonal tax administration. In early 2018, Hugo Wyler was appointed head of the Communication Section, which is now directly responsible to the Commissioner.

The FDPIC exercises his statutory duties as a supervisory body autonomously. However, the Federal Chancellery supports the FDPIC by providing logistical and administrative services in line with the general standards of the Federal Administration. For example, the Federal Chancellery supported the FDPIC in successfully introducing the new Acta Nova records and process management system in September 2018.

Information services

Improvements to Information services were made in selected areas during this reporting period. This concerns this report in particular. . However, developing content and the publication channels is a long-term task which we must achieve with limited resources (cf. Chapter 3.2 of this report).

Proceedings under the Freedom of Information Act (FoIA)

After a one-year trial, the FoIA has begun to follow a faster, abbreviated procedure in which disputes are normally settled orally. This procedure has proven to work well in that the proportion of disputes settled amicably remains high and statutory time limits were only exceeded in cases where the procedures and content were complicated. Such cases involve, for example, particularly challenging legal, technical and political questions, large numbers of documents or cases where third parties have to be involved in proceedings.

digital processing methods and technologies were used to identify them.

Federal Data Protection and Information Commissioner

15

1.1 Digitalisation and fundmental rights

Revision of the Federal Data Protection Act (FADP)

There is still no indication as to when the Federal Assembly's deliberations on the complete revision of the 1992 Data Protection Act will be completed.

On 15 September 2017, the Federal Council presented a complete revision of the Federal Act on Data Protection (FADP) with an accompanying report to the Federal Parliament (dispatch 17.059) to the Federal Assembly. In its deliberations on the FADP revision, the National Council's political institutions committee decided in a first step only to deal with the amendments required to adopt the Schengen acquis. These provisions, which relate solely to the federal prosecution authorities, were approved by Parliament and brought into force by the Federal Council on 1 March 2019 (see Schengen Data Protection Act, Sec. 1.2).

In contrast, the abovementioned committee has not yet concluded its deliberations on the complete revision of those parts of the FADP that apply to all the other federal authorities and enterprises and to the entire private sector. As this report went to press, there was still no indication as to when the National Council would consider the bill in plenum (see point I and Chapter 1.9).

Data protection guidelines in the context of elections and votes

In the reporting year, the FDPIC, together with the cantonal data protection authorities and experts, drafted guidelines on the processing of personal data in connection with elections and votes.

Working with the Conference of Swiss Data Protection Commissioners (privatim), and in close consultation with the Federal Chancellery, the FDPIC set up a working party tasked with raising public awareness of the systemic risks of personal data processing in connection with elections and votes. This working party, comprising data protection professionals as well as a political scientist, interviewed various experts during the year under review. The insights were set down in guide-

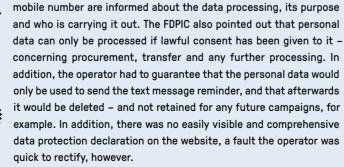
lines that are intended as an interpretation aid for the various political opinion-makers when applying the FADP (which dates back to 1992) to data processing in the context of elections and votes in the dynamic environment of digitalisation.

Unlawful data procurement in the run up to a vote

In the run up to the vote on the so-called Self-determination Initiative in November 2018, an agency obtained personal data unlawfully via a website. After we intervened, the agency changed its practices.

The website 25november.ch allowed individuals to enter up to ten mobile phone numbers along with the surnames and first names of their family, friends and relatives. These people were then sent a text message on the weekend of the vote on the Self-determination Initiative – ostensibly sent by the person who had entered the mobile phone numbers on the website and had thus given these details to a third party. The FDPIC stepped in and sent a letter to the operator of the website, requesting the agency to ensure that everyone who has provided details of their







The guidelines call upon those opinion-makers to be as transparent as



possible with voters and allow them maximum self-determination, using apps which are privacy-compliant. Anyone

who processes data in the context of elections and votes must be aware that, under data protection law, information about political and ideological views is subject to a higher level of protection than similar data in the commercial sphere. The guidelines are aimed at all political opinion-makers, such as parties and stakeholder groups, data traders and data platforms, and exhort them to make voters aware – and give them a proper understanding of – digital processing methods.



Systematic use of the OASI number by the authorities

The Federal Council is keen to facilitate wider use of the OASI number and, on 7 November 2018, launched a consultation on the amendment of the OASI Act. The consultation process lasted until 22 February 2019. We took the opportunity to share our preliminary remarks, which were incorporated in the draft law.

Under the draft issued for consultation by the Federal Council, the federal, cantonal and communal administrations would be authorised to routinely use the Old Age and Survivors' Insurance (OASI) number as a unique identifier even for purposes other than social insurance.

We are pleased that, based on our comments, the Federal Council's bill now expressly requires entities which hold databases in which the OASI number is routinely used to periodically carry out risk analyses, taking particular account of the risk of unauthorised



data matching and that, based on this risk analysis, state-of-the-art security and data protection measures must be defined and

implemented which are commensurate with the risk situation. 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. Finally, we underlined the

necessity to introduce more stringent technical and organisational measures.

The Federal Social Insurance Office has written to the FDPIC to confirm that the 'Security Plan for Personal Identifiers' which the National Council Legal Affairs Committee called for by the end of 2019 in postulate 17.3968 will be included in the dispatch as part of the legislative work on Old Age and Survivors' Insurance. The aim of this security plan is to demonstrate how to counter the risks of systematic usage of the OASI number as an unambiguous identifier of an individual and to show how data protection can be improved.

We remain very much in favour of the use of sectoral personal identifiers. This would considerably reduce the risks inherent in using unique identifiers, particularly unlawful linkage between separate databases and information systems. In that respect, we can also deduce from the draft issued for consultation that it should be possible to maintain the requirement of sectoral personal identifiers rather than the OASI number in special legal provisions for certain purposes, including for the electronic patient record.

Parameters for a Swiss data policy

The office consultation procedure provided an opportunity for the FDPIC to comment on the parameters of a Swiss data policy. He is still addressing certain aspects of data policy.

During the office consultation procedure, the FDPIC made the general point that data protection regulations must be observed not only for Open Government Data (OGD), but also in other areas listed. These are: management of master data by the Confederation, data of federal businesses and research institutes, data innovation in statistics and innovation using data in the sphere of mobility and health. Moreover, the risk that, depending on the volume of data available, data subjects could still be identified is ever-present with anonymised data, hence data protection must also be observed. The FDPIC also stated that. since the office consultation on the FADP, he has advocated the introduction of a right to data portability. The FDPIC's comments were incorporated.

A number of digitisation and data policy projects, coordinated by OFCOM, are currently underway at federal level. The FDPIC is actively involved in some of them, including a project on the use of data and the sub-working group tasked with looking at data availability.

Advisory Council on Digital Transformation

In March 2019, the FDPIC took part in the sixth meeting of the 'Digital Transformation' advisory board run by EAER and DETEC. The purpose of the board meetings is to highlight concrete examples of digital transformation projects and how they benefit the economy and society. The 'Swiss Data Custodian' project aims to create a system for storing confidential data. The intention is for the custodian to be sent personal and other raw data from different companies – and possibly from public administration offices too, to analyse these data using artificial intelligence and then finally make the results available for commercial purposes in anonymised form. Applications in transport, medicine and humanitarian work are currently under discussion. The FDPIC attended the preparatory meetings and the board meetings and used both opportunities to present the data protection frameworks and requirements which need to be taken into account. The FDPIC will continue to support the project.

Data linkage for statistical purposes

Linking data enables new insights to be gained from statistical databases.

Data linkage can significantly increase the risk of re-identification. To combat this, the FSO has issued regulations on data linkage.

The Federal Statistical Office (FSO) is permitted by law to link data. Linking data from various surveys is a valid statistical tool for gaining new insights from existing databases, observing trends over a number of years or making projections. It involves allocating identification numbers to the individual datasets in the various databases, then generating a linkage identifier.

In data protection terms, data linkage carries the risk of enabling identifiable individuals to be traced; this is called re-identification. Because of this, the internal management processes for ID numbers and identifiers must preclude such traceability and prevent any abuses. The FDPIC asked the FSO for information about current and planned linkage projects and measures to protect personal rights. Clearly, this is a highly complex issue which the FDPIC will continue to monitor. We welcome the fact that the FSO has issued and published specific linkage regulations.

21

Focus I Focus I

Electronic proof of identity (E-ID)

An officially-recognised electronic ID will be used to establish a person's identity in electronic applications. The FDPIC is monitoring this large-scale digital project on all levels. As a top priority, he is demanding safeguards of adequate data protection.

Legal certainty and trust are essential to doing business. For various processes, establishing the counterparty's identity is of paramount importance. For the analogue realm, the Confederation makes conventional means of identification available – i.e. the Swiss passport, ID card and foreign national identity card. Now that business processes are shifting to the digital realm, different requirements apply to establishing identity. In addition to the conventional means, individuals will be able to prove their identity by means of an officially recognised electronic identity (E-ID).

The E-ID will be a key instrument for online access to major private services – such as opening a bank account - as well as e-government applications, including ordering an excerpt from the register of criminal convictions. For this reason, the FDPIC has always kept a critical but positive eye on both the legislative project for an officially recognised E-ID and the actual implementation of the project at SwissSign Group AG (see also Chapter the "Swiss ID" below) and has called for key data protection requirements to be incorporated during the project concept phase.

On 1 June 2018, the Federal Council adopted the dispatch on the Federal Act on Recognised Electronic Means of Identification (E-ID Act, BGEID), which sets out the legal framework for the officially recognised identity. The bill was approved by 128 votes to 48 by the National Council at the end of March.

Officially recognised private companies to act as identity providers

After consulting the interested groups, the National Council, through its Legal Affairs Committee, declared its opposition to a state-only solution, advocating instead a division of tasks: officially recognised private companies, known as Identity Providers (IdP), will be authorised to issue electronic identities. IdPs will be recognised by the Federal IT Steering Unit (FITSU), which will also check compliance by the IdP with the specified processes and technical standards and, based on that check, issue, renew or withdraw recognition. An electronic interface operated



by the Federal Office of Police (fedpol) will make personal identification data stored in registers maintained and updated by the state available to the IdPs for the sole purpose of identification. The intention is that this divi-

sion of tasks will guarantee a reliable framework which safeguards security and can be enforced by government institutions during recognition and supervisory procedures. Furthermore, the technical implementation and marketing of the actual E-ID can be left to private enter-

Consulting the FDPIC: a condition for recognition

At the hearing on the Committee, the FDPIC felt that, irrespective of the political decision in favour of a state-only or part-state solution, his task was to ensure the highest possible level of data protection. The FDPIC made it very clear that there must be a proper legal basis for data processing by state actors and demanded improvements to specific aspects of the E-ID Act in this regard. As regards the FDPIC's call for contemporary data protection for private actors, the National Council included in the Act the requirement that FITSU must first consult the FDPIC as a condition for recognising IdPs. The FDPIC will demand that the data protection standards which he drafted when overseeing the SwissSign project (see below) serve as the basis when assessing eligibility as an IdP.

Furthermore, the FDPIC insisted that the ambiguous dispatch be reworded to make it clear that the E-ID is only



to be used when business transactions require secure identification. The E-ID Act may not **DDD** create new identification obligations, for either analogue or electronic business transactions, for the numerous purchases of goods or services for

which this is not necessary. The National Council amended the relevant article of the Act accordingly. Focus I

The "SwissID"

A private provider is developing the "SwissID" as an electronic identity. The FDPIC is keeping track of the project at regular meetings with the project managers, who have taken the FDPIC's suggestions under consideration.

SwissSign Group AG – a joint venture of federal enterprises, finance companies, insurance companies and health insurance funds – is introducing its product "SwissID" as an electronic identity for online commerce on a private basis and on various online platforms. The contractual partners in SwissSign's online service include major companies such as Swiss Post, Swisscom, Coop and Ringier, and others such as SBB are continually joining their ranks. A number of cantons are either planning to use, or have already introduced, the "SwissID" for their e-government applications.

At present, the "SwissID" is still based on a login password process. However, with a view to the entry into force of the BGEID (Federal Act on Recognised Electronic Means of Identification; see also the article on the E-ID), it will be upgraded to an electronic identity on a private basis so that users can conclude private legal transactions online and procure government services online.

More extensive analyses of data protection risks required

This project is also a significant, large-scale digital project from a data protection perspective. The FDPIC is in regular discussions with the project managers, advises them on specific issues and gives feedback on the documentation and information presented to him. Clearly, SwissSign is aware of the importance of data protection in its data processing operations and has taken essential technical and organisational measures to protect data. However, the FDPIC has pointed out that the analyses of data protection risks that are typically associated with the project



must be deepened and appropriate measures should be taken to prevent those risks.

Moreover, we consider it vital that an officer be appointed specifically for operational data protection and be tasked with regularly

reviewing the risks and the corresponding measures, and commenting on decisions made by the company from a data protection perspective.

The project managers at SwissSign agree with the FDPIC's points and will broaden out their analyses and documents pertaining to the processing of personal data. A company data protection officer has been designated by the company.



1.2 Justice, Police, Security

Police counterterrorism measures

During the second office consultation procedure on the draft Federal Act on Police Counterterrorism Measures, the FDPIC again issued a large number of comments. He reiterated his demand for consistent legislation at federal level and called for restrictions on access by migration authorities to police databases.

The FDPIC once again criticised the large number of laws governing the activities of the Federal Police. Moreover, police data is processed in a disorganised way, in several databases and in a growing number of applications. The latest draft Federal Act on Police Counterterrorism Measures (PCTA) aggravates this situation. Consequently, the FDPIC repeated his demand for consistent legislation to be introduced at federal level, like that in place in the cantons. He also reiterated the importance of a clear division of competencies between the Federal Intelligence Service (FIS) and fedpol.

Furthermore, the FDPIC questioned whether there is any practical need for the State Secretariat for Migration (SEM) to access the information systems mentioned in Articles 10, 11, 12 and 14 of the Federal Act on the Federal Police Information Systems (FPISA). The legal framework set forth in the laws on foreign nationals and asylum pertain only to collaboration and coordination between the SEM and fedpol. These provisions are not a legal basis that confers upon the SEM an explicit legal mandate in the detection of terrorist acts and counterterrorism. Moreover, the data being accessed is that held by the criminal police or relating to crime analysis. Such data is highly sensitive and some of it is not yet confirmed. Access to such data by the migration authorities must be obtained through the system of mutual assistance in administrative matters, not online. This would enable fedpol to keep the dissemination of this data to a bare minimum.

Lastly, the FDPIC also stated that consulting the computerised police search system (RIPOL) will not enable the transport police to fulfil its lawful task, i.e. checking a person's identity or identifying an individual. In fact, RIPOL flags up whether an alert applies to a particular individual. Such access to RIPOL would require the proposed amendment to the Federal Act on the Federal Police Information Systems as well as the Federal Act on the Security Units of Public Transport Companies.

Certain improvements to the Swiss-U.S. Privacy Shield required

The review of the EU-U.S. Privacy
Shield and, for the first time, of the
Swiss-U.S. Privacy Shield was conducted in Brussels in autumn 2018.
The U.S. authorities addressed various
concerns and made a number of
improvements which will also benefit
Switzerland. There is, however, still a
need for coordination of HR data,
among other things.

Two cases concerning companies which falsely claimed to be certified under the Privacy Shield were reported to the FDPIC in the year under review. Both claims were resolved in cooperation with the Department of Commerce (DoC) see also point 1.4 of the report on the first Swiss-US Privacy Shield Review). In addition, data subiects from Switzerland have filed around ten legitimate complaints with an Independent Recourse Mechanism (IRM) provider. No case relating to the ombudsperson mechanism, which aims to remedy the authorities' access to personal data, has been reported to the FDPIC.

It seems reasonable to conclude that the legal instruments made available by the Swiss-U.S. Privacy Shield have been little used so far. It should be noted, however, that the Swiss agreement has only been in force since April 2017, and that before an official complaint is filed, the certified company itself is usually the first to be approached. It can be assumed that an indeterminate number of data breaches have already been remedied in this way.

Initial review by the FDPIC

The review of the Privacy Shield covered both the commercial aspects (e.g. supervision and enforcement of the obligations of certified companies) and the authorities' access to personal data for national security purposes. Switzerland was able to attend the previous European review of the EU-U.S. Privacy Shield as an observer. Topics concerning both the Swiss-U.S. and the EU-U.S. Privacy Shield were discussed exclusively at the EU-U.S. review. The knowledge gained could also be used for the Swiss-American agreement.

Since the adoption of the Swiss-U.S. Privacy Shield, various improvements have been made. As regards the commercial aspects, the U.S. Department of Commerce has, among other things, stepped up its search for false claims. In addition, the U.S. authorities regularly check correctly certified companies for any weaknesses, and monitor certification more closely to avoid any discrepancy between the information in their privacy policies and the state of progress of the registration process.

Five additional arbitrators for Switzerland were already appointed prior to the review for the arbitration proceedings which are available to the data subjects upon exhaustion of other legal remedies (IRM) at an arbitral tribunal subject to American law (cf. Activity Report No 24 of 2016/2017, point 1.8.1). These additional arbitrators supplement the EU list (Hyperlink).

With regard to official access to personal data, progress was made in the run-up to the review. The U.S. Senate confirmed the nominations of the chairman and two members of the Privacy and Civil Liberties Oversight Board (PCLOB), thus constituting the necessary quorum. In the first year of the Swiss-U.S. Privacy Shield, the PCLOB had only one member and was therefore not quorate.

Room for further improvement

In a variety of sectors, the FDPIC shares the view of the European Data Protection Board (EDPB) that further improvements are needed. Among other things, it would make sense for the U.S. authorities to conduct more substantial reviews on the compliance of certified companies, including reviews on the purpose and proportionality of data transfers to third parties. A solution also needs to found on how to interpret the term 'HR data', which at present is not interpreted consistently by the U.S. authorities on the one hand and the FDPIC and representatives of the EDPB on the other. HR data benefit from greater protection under the Privacy Shield agreement. According to the FDPIC, the interpretation of this term needs to be broader than the DoC's interpretation.

With regard to the authorities' access to personal data, improvements should include appointing an ombudsperson who has the necessary powers and independence vis-à-vis the U.S. authorities who access personal data within the framework of national security.

Although weaknesses were identified in the review, the overall functioning of the Privacy Shield has improved since it came into effect.

Release of airline passenger data in EU states

A number of EU states are planning to request airline passenger data for flights from Switzerland. There is currently no legal basis for them to do so, but a planned ordinance could provide one.

In the spring of 2018, a meeting was held between the Federal Office of Civil Aviation (FOCA), the Federal Office of Justice (FOJ), Federal Office of Police (fedpol) and the FDPIC on the release of airline passenger data (PNR information) in member states of the EU. This meeting was suggested by the FOCA, as airline companies had been informed by various EU states of the those states' plans to request that PNR data be provided for flights from Switzerland on the basis of the EU PNR Directive of 27 April 2016 (Directive (EU) 2016/681; EU PNR Directive) on the use of passenger name record (PNR) data for the prevention, detection, investigation and

prosecution of terrorist offences and serious crime. However, the EU has stated that the EU PNR Directive is not relevant to Schengen and, as such, does not have to be automatically adopted by Switzerland.

The FDPIC pointed out that the release of PNR data by airlines in the form of an agreement must have a legal basis. While the other federal offices concerned were very much in favour of unconditionally releasing the data, the FDPIC insisted that data must only be released to member states by airlines, in implementation of the EU PNR Directive, if certain requirements are met. Switzerland must seek as soon as possible to negotiate and obtain an association to the EU PNR Directive. With this in mind, fedpol originally planned to submit the relevant bill to the Federal Council in autumn 2018, along with a mandate for negotiations with the EU. However, this project has been put on hold until further notice. When the FDPIC learned of its postponement, he made the federal offices concerned aware that an alternative legal basis would have to be established as quickly as possible. The FDPIC was assured that the legal basis for the delivery of PNR data to states which demand the data pursuant to the EU PNR Directive would be created by revising the Air Navigation Ordinance (ANO), to the effect that data may only be released to states

which demonstrate an adequate level

oversee the legislative work in an advi-

of data protection. The FDPIC will

sory capacity.

'Swiss' booking system -Calls for measures to prevent data misuse

Swiss International Air Lines is taking a number of additional measures to prevent any abuses when retrieving bookings via its website.

It was brought to the FDPIC's notice that, by entering last name, first name and booking number when logging in to the 'Swiss' website, it is possible to retrieve a variety of personal data (first name, last name, date of birth, gender, nationality, place of residence, number and validity period of passport or ID card). It is very easy to find out the last name, first name and booking number of other passengers on boarding cards which they leave behind, throw away or publish on social media after a flight. This information could also be read from the barcode on the boarding card, using a simple barcode reading app. By logging in, it is also possible to view all bookings made by the passengers concerned and amend some data.

As the content of the boarding pass, including QR code, must satisfy certain international standards, it cannot simply be altered by individual airlines. Nonetheless, airlines must and can take the necessary measures to ensure that passenger data is adequately protected in the booking system against any improper processing.

The FDPIC held discussions with Swiss and the additional measures necessary to prevent any abuses identified. Swiss has revised its General Conditions of Carriage to make its customers more aware of how important it is to protect the personal data that is visible/stored on the boarding pass. Furthermore, after using the automatic check-in, customers receive a warning about this by e-mail. If they check-in online, the address (e-mail, mobile phone number) to which the message will be sent is also shown, to make sure that the boarding card is sent to the correct/requested address. In addition, the passport number – which, in certain cases, is displayed when the booking is retrieved – should be partially obscured. The FDPIC also suggested that, when retrieving bookings not made through a travel agency



or another third party but directly via the airline's website, an element such as mobile phone number or e-mail address should be

provided in addition to the name and booking reference. Discussions on this point were still ongoing at the end of the reporting year.

Approximately 2900 U.S. companies certified

The Swiss-U.S. Privacy Shield has been in force since 2017. The Privacy Shield allows U.S. companies to process personal data from Switzerland without any further data protection obligations. The companies can become certified for the programme by the U.S. Department of Commerce and thus commit to comply with an adequate level of data protection under Swiss law. Data subjects have mechanisms at their disposal for protection against a data breach (cf. our Activity Reports Nos 24 and 25, point 1.8.1 in both reports).

By February 2019, 2,883 U.S. companies had become certified under the Swiss-U.S. Privacy Shield, including Facebook, Microsoft (with 27 subsidiaries) and Google.

Certified companies can largely choose to comply with the Independent Recourse Mechanism (IRM) under the Alternative Dispute Resolution body (ADR) or under the FDPIC (see Guide to the Swiss-U.S. Privacy Shield).

SECO (lead) and the FDPIC, together with the U.S. supervisory authorities conduct an annual review of how the agreement is working.

28

Focus II

Schengen Data Protection Act in force

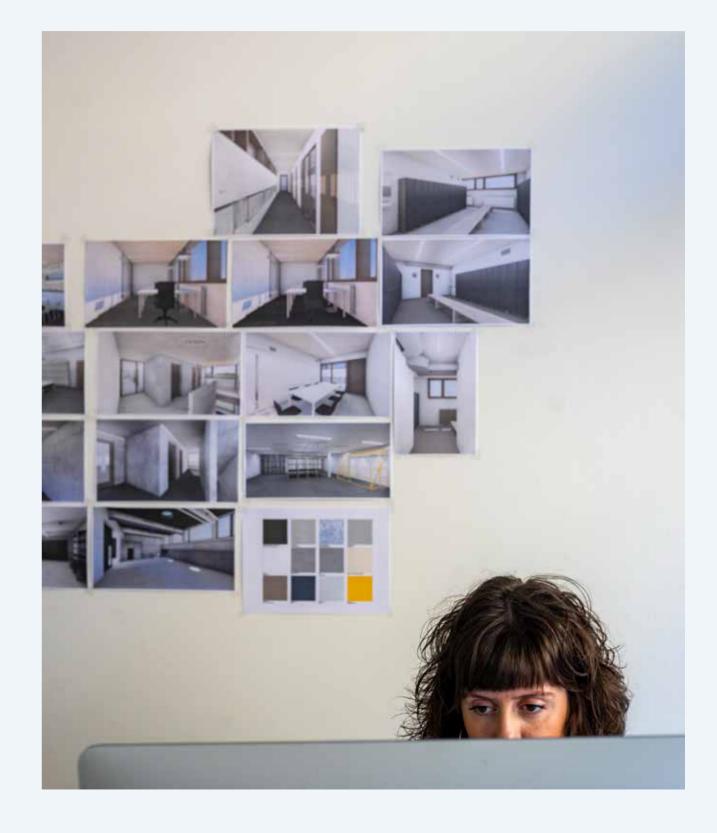
The Schengen Data Protection Act (SDSG) took effect on 1 March 2019. It adds a number of new powers to the existing ones exercised by the FDPIC. Among other things, it authorises him to investigate and issue rulings in criminal matters, in application of the Schengen acquis.

When debating the revision of the Data Protection Act (FADP), parliament decided to begin by discussing the changes necessary in order to incorporate the Schengen acquis. Based on this, the Federal Act on the implementation of Directive (EU) 2016/680 was adopted. This took effect on 1 March 2019. Firstly, the Act introduces the Schengen Data Protection Act (SDSG) and, secondly, it revises various acts which apply in the sphere of Schengen cooperation in criminal matters.

The SDSG applies in particular to the processing of personal data by federal bodies in criminal matters, within the context of the application of the Schengen acquis. Besides the Federal Office of Police (fedpol), the FOJ (which handles international mutual legal assistance in criminal matters) and the Office of the Attorney General of Switzerland, those federal bodies also include the Federal Criminal Court, the Federal Supreme Court and the cantonal compulsory measures courts, if they are engaged in the service of the Confederation. The SDSG does not apply to cantonal authorities. Instead, the Cantons must bring their legislation into line with the new EU requirements wherever necessary.

The main changes under the SDSG are as follows:

- genetic and biometric data which unambiguously identify a person will now be explicitly listed as sensitive personal data;
- in line with European law, the term "profiling" replaces
 "personality profile". Profiling denotes any kind of automated processing of personal data which involves using
 that data to evaluate particular characteristics pertaining
 to an individual. In particular, it is used to analyse or predict aspects relating to the individual's work performance,
 financial situation, health, personal preferences, interests,
 reliability, conduct, whereabouts or change of location.
- "Privacy by design and default" is enshrined as a principle.
 In order to demonstrate compliance with data protection regulations, the federal body must take the necessary internal precautions and introduce measures which satisfy this principle.
- specific rules are laid down for automated individual decisions. A decision is automated if the evaluation of the data and the ensuing decision are not undertaken by a natural person i.e. when the machine decides, not a human:
- if the proposed data processing might present a substantial risk to the fundamental rights of data subjects, federal bodies must carry out data protection impact assessments and, if necessary, consult the FDPIC;
- If the federal body has undertaken a data protection impact assessment in accordance with Article 13 SDSG, the results must be taken into account when devising the measures;
- federal bodies must notify data breaches to the FDPIC;
- the FDPIC can now issue rulings as an administrative measure.



Focus II

Schengen evaluation of Switzerland - sufficient resources required

Switzerland's implementation and application of the Schengen acquis as an associated member was evaluated for the third time in 2018. Experts from the other Schengen countries and the European Commission chiefly addressed the application of the Schengen rules on data protection. Based on the findings, the EU Council sent its recommendations to Switzerland.

The evaluation, which is carried out at intervals of five years at the most, covers all areas of Schengen collaboration: management of external borders (airports), return/repatriation, Schengen SIS II/SIRENE information system, common policies on visas, police cooperation and data protection.

Work to prepare for and carry out the evaluation was coordinated by the Federal Office of Justice (FOJ), in collaboration with the Directorate for European Affairs (DEA). The FDPIC was actively involved in the Schengen data protection evaluation – in collaboration in particular with the FOJ, the Federal Office of Police (fedpol), the State Secretariat for Migration (SEM), the Federal Department of Foreign Affairs (FDFA) and the cantonal data protection authorities (see the section on Cooperation with the cantons No. 1.9). The Federal Office of Justice is responsible for coordinating all evaluations.

32

There were three stages to the data protection evaluation procedure. During the first stage, Switzerland had to answer around 200 questions on the implementation and application of the Schengen rules and set out the main legislative and operational changes made since the last evaluation. The second phase involved local inspections in Switzerland. Experts from other Schengen countries and the EU checked, in situ, that Switzerland is correctly implementing and applying the Schengen provisions on data protection. They visited from 26 February to 2 March 2018 and focused on data protection legislation as well as the competencies of the FDPIC, the Lucerne data protection authority and other federal bodies (see above). Particular attention was paid to the supervisory, investigative and intervention powers of the supervisory authorities and their independence. The legal bases and, specifically, the powers of oversight over SIS II and VIS and the services involved in its management were analysed. The rights of data subjects, data security, cooperation with foreign authorities and public information were also evaluated.

Based on the results of the evaluation am 7 March 2019 the EU Council decided to make a recommendation to Switzerland on the elimination of the deficiencies identified. With regard to the FDPIC, the Council recommends in particular that he should check the legality of the processing of personal data in connection with Schengenrelated information systems more frequently. In order to fulfil all his duties in terms of the SIS II and VIS acquis, the FDPIC should be allocated sufficient financial and staff resources. In addition, the FDPIC should have genuine influence over his proposed budget, with Parliament being informed about the proposed budget for the FDPIC when it is considering the overall budget proposal. In its considerations, the Council also recognises certain positive aspects, such as the guide to the "Supervision of the use of the Schengen Information System (SIS)" produced by the Swiss data protection authorities' Schengen coordination group or the highly comprehensive and specific sample letters available to persons wishing to exercise their rights, and the excellent information that can be found on the FDPIC website. It urges Switzerland to draw up a plan of action within three months of accepting the decision and to submit this to the Commission and the Council. The next evaluation is planned for 2023.

Data protection Data protection

Automated vehicle searches and traffic surveillance

Police and customs authorities will be able to use the new modules and new functionalities of the new automated vehicle search and traffic surveillance system if, with regard to data protection, there is an adequate legal basis for them to do so.

The Federal Customs Administration (FCA) and the cantonal police have been using automated vehicle search and traffic surveillance systems for more than a decade. The Swiss Police Commission is planning to replace the software (AFV Redesign) and introduce new modules and new functionalities. In view of this, a review of the requirements and legal framework was conducted. The FDPIC and privatim participated in an ad hoc working group. Users of these automated systems would like to be able to use new modules and new functionalities. Such usage is possible only with the appropriate legal basis.

Furthermore, the principle of proportionality must be fully observed. This analysis is based on the number of



cameras, their positioning, the utilisation of the data, the way in which the search data is used, how it is communicated, etc. In the can-

tons, the checks generally take place during the prior consultation procedure with the data protection authority. At Confederation level, observance of the principle of proportionality is checked during the office consultation on a legislative proposal.



1.3 Taxation and finance

Release of personal data to foreign tax authorities

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.

a) 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. Now, the Federal Council wants to add, at the last count, 18 additional partner states to the Swiss AEOI network, with which the AEOI will be implemented from 2020/ 2021. (Further information is available on the website of the Federal Department of Finance.)

As with previous office consultations, in the current reporting year the FDPIC once again pointed out that, if the AEOI is to be introduced with additional partner states, it is essential to guarantee an adequate level of data protection in each state. Our list of countries contains an adequacy rating for each individual country. During an office consultation held at the start of November 2018 concerning the introduction of the AEOI with additional partner states from 2020/21, we commented that none of the proposed partner states with which the AEOI is to be implemented on a reciprocal basis (including Albania, Azerbaijan, Brunei Darussalam etc.) have an adequate level of data protection (see Art. 6 para. 1 FADP) and, consequently, adequate data protection must be assured by sufficient safeguards (see Art. 6 para. 2 FADP). In this regard, the Federal Council invoked the communication issued on the basis of the Multilateral Competent Authority Agreement (MCAA) and sent by Switzerland to the coordination committee on 4 May 2017, laying down data protection safeguards which must also apply to taxpayers in the partner states. However, in the FDPIC's opinion, this communication does not constitute a sufficient safeguard in accordance with Art. 6 para. 2 (see 24th and 25th Annual Report, section 1.9.1 a). Therefore, the plan to add more states presents problems from a data protection perspective.

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

During an office consultation the year under review, the FDPIC again commented on the list of countries for the activation of the exchange of country-by-country reports (see also 24th and 25th Annual Report, Section 1.9.1). He pointed out that the latest proposed addition of eight more states and territories (including the United Arab Emirates, Serbia and Zambia) involves states which are listed on the FDPIC's list of countries as having an inadequate level of data protection. Therefore, the FDPIC reiterated that, with regard to such countries, additional safeguards in accordance with Art. 6 para. 2 FADP are necessary to ensure an adequate level of data protection.

c) Relaxation of international administrative assistance on tax matters in the event of data theft

In the year under review, during an office consultation the FDPIC once again addressed Art. 7 let. cTAAA, which concerns the exchange of information at the request of a foreign state and sets out the cases in which such requests are not considered. As the law stands, a request will not be considered if "it violates the principle of good faith, particularly if it is based on information obtained through a criminal offence under Swiss law". In the past, the FDPIC had stated that, in his opinion, whether the requesting state obtained such information passively (e.g. as a result of spontaneous administrative assistance) or actively was immaterial; in either situation, the state which accepts the stolen data offered by it is acting unlawfully (see Section 1.9.3 of our 23rd Annual Report).

This viewpoint is in line with the practice that has prevailed until now but has been criticised as overly restrictive by the Global Forum on Transparency and Exchange of Information for Tax Purposes. A decision since made by the Federal Supreme Court (judgment 2C 648/2017 of 17 July 2018) found that, in principle, requests that are based on data of criminal origin may be considered as long as the requesting state has not bought the data with the intention of subsequently using it for an administrative assistance request. Therefore, Art. 7 let. c TAAA will now stipulate merely that a request will not be considered if it violates the principle of good faith. In light of the judgment of the Federal Supreme Court, which must be respected, the FDPIC did not raise any objections.

Objection against FDF in the FTA case still pending

The recommendation issued by the FDPIC at the end of 2017 concerning information about names openly disclosed in international tax-related administrative proceedings was not supported by the Federal Department of Finance (FDF). The FDPIC filed a complaint with the Federal Administrative Court against the FDF's negative decision.

At the end of December 2017, we issued a formal recommendation that, in international tax-related administrative assistance, the Federal Tax Administration (FTA) should also inform in advance persons not formally affected but whose names are to be openly, i.e. in unredacted form, transmitted to the foreign authority making the request (see Section 1.9.2 of the 25th Annual Report of the FDPIC). The FTA rejected this recommendation and the FDPIC then exercised his legal option to refer the matter to the competent department.

In its decision of 20 September 2018, the Federal Department of Finance (FDF) supported the FTA's stance that the FDPIC's recommendation to inform third persons whose names are to be openly transmitted in administrative assistance proceedings would be too costly an exercise and would render effective administrative assistance impossible. The argument was that data subjects' rights were already taken into account, because only the bare minimum of data is transmitted. Consequently, it rejected the FDPIC's request.

Informing third parties need not incur excessive expenditure

The FDPIC stands by his opinion that third persons must have the option of asking the courts to assess whether, in a specific, individual case, the open transmission of their name is permissible. This is the only way to ensure that their constitutional rights are preserved. In order that the necessary legal steps can be instigated, data subjects must be informed of the planned transmission. Moreover, the FDPIC assumes that the time and cost expenditure involved in informing



them can be kept within reasonable boundaries by suitable technical and organisational measures, so that it does not pre-

clude effective administrative assistance. Therefore, on 5 October 2018 he filed an objection to the FDF's decision with the Federal Administrative Court. At the end of the year under review, the case was still pending.

Recommendation against Zentralstelle für Kreditinformation (ZEK)

Loan applications which are rejected for reasons that bear no relation to the applicant's creditworthiness or borrowing power must be erased from the database as soon as they are rejected. The FDPIC made a recommendation to this effect to the credit information agency Zentralstelle für Kreditinformation.

The Zentralstelle für Kreditinformation (ZEK) collects credit rating information from lending transactions involving individuals and legal entities and makes it available to its members, in particular banks, for a fee. During the last reporting year, we initiated a case investigation at the ZEK (see also Section 1.8.12 of the 25th Annual Report of the FDPIC). Based on reports received from members of the public as well as media coverage, the FDPIC identified potential shortcomings relating to privacy compliance in the processing of requests for information, the rectification and erasure of data, measures to prevent improper enquiries and the technical and organisational separation of the ZEK's databases from those of the consumer credit information agency Informationsstelle für Konsumkredit (IKO). The latter has concluded a licence agreement with the ZEK for the use of its information system.

However, our investigations found that the ZEK is privacy-compliant in the areas investigated. Requests for information, rectification and erasure are processed correctly, measures to prevent improper enquiries satisfy the relevant requirements, and the technical and organisational segregation of the ZEK and IKO databases is sufficient.

Recommendation on inappropriate data storage

The FDPIC made just one recommendation, pertaining to the rejection of loan applications and card applications. He noted that loan and card applications which are refused for reasons that bear no relation to the applicant's creditworthiness or borrowing power (e.g. the credit quota for a specific period has been exhausted) are kept in the ZEK's database even after the application is rejected, even though this information is irrelevant to evaluating lending decisions – and, by



extension, to the purpose of the database. Therefore, the FDPIC recommended that such entries be erased from the ZEK database as

soon as the application is rejected.

The ZEK accepted the FDPIC's recommendation and will make the necessary changes to its regulations and in the database. The FDPIC was thus able to conclude the proceedings without imposing any further measures.

Data protection Data protection



1.4 Commerce and economy

Data theft case at Swisscom concluded without formal action being taken

At the end of 2017, Swisscom informed the FDPIC about a data theft. Most of the people affected were private owners of mobile phone numbers. The FDPIC was able to conclude the procedure carried out at Swisscom to review potential risks of consequential losses caused by the reported data theft, but without making any formal recommendations.

At the end of December 2017, Swisscom notified the FDPIC that, in the autumn of 2017, the contact data of around 800 000 customers were accessed without authorisation. Most of the people affected were private owners of mobile phone numbers, along with a few landline customers. Shortly after that, an incident of alleged unauthorised access to the data of a Swisscom customer was reported to the FDPIC. There was, however, no causal connection with the reported data theft (see also the 25th Annual Report of the FDPIC, Section 1.3.1). However, following a report of improper access to customer data which was potentially connected with a data theft at Swisscom which became public knowledge at the start of February 2018, on 9 February 2018 the FDPIC initiated a procedure and requested information from Swisscom in connection with the risk of consequential losses (see also Section 1.3.2. of the 25th Annual Report of the FDPIC). In response, Swisscom submitted documentation about the suspected cases reported to it and the measures taken in each instance. In each of the cases dealt with, there was

a suspicion that the stolen data might be used to gain unauthorised access to other customer data.

Based on the documentation provided, the FDPIC investigated whether the measures taken by Swisscom in connection with the data theft afford adequate protection for data subjects or whether the reported suspicious cases reveal the need for further mea-

Even after in-depth examinations, no connection could be identified in any of the investigated cases with the data leak in question. The incidents could all be attributed to technical



errors or faulty operations. Since Swisscom took measures to rectify the error and prevent similar incidents in future, the FDPIC was able

to conclude the procedure without any formal action being taken.

After the data leak was published by Swisscom, the FDPIC received a request for access to the documents concerned under the Freedom of Information Act. Having consulted Swisscom, the FDPIC decided that access should be granted, with the exception of the personal data contained in the documents, and issued a ruling to that effect. Swisscom filed an objection to that ruling with the Federal Administrative Court. At the end of the year under review, the case was still pending.

Data theft at EOS storage of unnecessary patient data

EOS replaced a system affected by data theft with a new system, whereupon the FDPIC concluded the case investigation.

At the end of December 2017, the FDPIC opened a case investigation at collection firm EOS Schweiz to clarify the data protection aspects of the suspected data theft, which had also been publicised in the media and mainly affected patients of Swiss doctors and dentists (see also Section 1.8.2. of the 25th Annual Report of the FDPIC).

Although the specific circumstances of the suspected data theft have yet to be conclusively clarified, the FDPIC's investigations revealed in particular that substantially more patient data than is necessary for invoicing or collection were being stored on EOS servers. Furthermore, the time limits for erasure were not met, resulting in a disproportionately large database.

EOS reached the same conclusions during its own investigations and has since replaced the system in question with a new one, rectifying the identified shortcomings. Therefore, the



FDPIC did not have to take any action and concluded the procedure without any formal recommendations. He reiterates that medical

personnel may only disclose patient data which are actually necessary for billing or collection purposes.

Use of ricardo.ch data within the Tamedia group

Auction site ricardo.ch shares its users' data within the Tamedia group, for security purposes and for targeted advertising. Since the opening of our formal procedure, ricardo.ch has revised its privacy statement and we are investigating whether the consent upon which the group bases its processing satisfies the legal requirements.

In July 2017, online auction platform ricardo.ch informed its users of a change to its privacy statement, bringing it into line with the statements of the Tamedia group companies, of which ricardo.ch is one. In particular, the new terms of use were to permit the sharing of data within the group – partly to allow targeted advertising but also to prevent potential abuses. If they did not respond, users of ricardo. ch were deemed to have agreed to the new privacy statement and, therefore,



to their data being shared with Tamedia and its affiliates. If they objected, their account was automatically closed or suspended. As we

had doubts as to the validity of the consent of data subjects, we opened a formal procedure to investigate whether the legal requirements in this regard were met (cf. Section 1.8.8 of our 25th Annual Report 2017/2018).

Since then, ricardo.ch has revised its privacy statement with effect from 25 May 2018, to coincide with the entry into force of the European General Data Protection Regulation (GDPR). From now on, ricardo users can object to their data being shared with the Tamedia group on their express request. We reviewed these new terms and based our investigation on them. In particular, we made sure that users are informed in a transparent and comprehensible manner about the processing of data concerning



them and that the consent required for targeted advertising satisfies the legal requirements. In order to be valid, consent

must be freely given, informed and – in the case of sensitive data or personality profiles – must also be explicit.

Case investigation at smart-TV manufacturer concluded

A procedure to clarify privacy compliance by a manufacturer of smart TVs when processing user data was concluded without any formal action being taken

The FDPIC carried out a case investigation at a manufacturer of smart TVs to ascertain which data the company processes about TV users, how those users are informed and whether they freely consent to the processing (see also Section 1.3.1 of the 25th Annual Report of the FDPIC). An in-depth analysis of the submitted documentation revealed that the manufacturer processes the user data in its possession in accordance with data protection regulations.

The manufacturer only processes personal data when technically necessary or when desired by the user due to specific additional functions. Otherwise, data is processed on an anonymous basis, e.g. for statistical purposes.

TV set users are informed about the possibility of data being transmitted to the manufacturer and how they will be



processed. They can completely prevent this and use the sets as conventional televisions, i.e. without smart TV functions. If the

smart TV functions are used, there is a technical need to process certain data; the scope of that processing cannot be restricted or prohibited by the user. However, the user can deactivate the processing of data purely for convenience or certain additional functions.

As the FDPIC found no instances of non-compliant data processing by the manufacturer, he concluded the procedure without taking any formal action.

Sporting goods retailer Decathlon - better information needed when gathering data

Decathlon made sales of goods in its Swiss stores contingent on the disclosure of customer data, prompting the FDPIC to initiate a case investigation. The retailer then made changes to its controversia practice.

During the reporting year, we opened a case investigation at sporting goods retailer Decathlon after learning from newspaper reports and notifications from members of the public and customer protection organisations that Decathlon 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. As the primary reason for the case investigation was thus resolved, the FDPIC concentrated its further investigations on the question of whether it is genuinely clear to customers that the provision of the information is voluntary.

The FDPIC's investigations revealed that the information provided by Decathlon is inconsistent and not always clearly worded, which may create the impression that the information originally deemed obligatory is still required in order to purchase



goods. He therefore made suggestions to the retailer for improvements to the information.

1.5 Health

Statistics project using insurers' individual datasets (BAGSAN)

The Federal Office of Public Health runs the BAGSAN statistics project using insurers' anonymised individual datasets. The FDPIC oversees the project, which has also given rise to political debate.

The FDPIC has been monitoring the BAGSAN statistics project run by the Federal Office of Public Health (FOPH) since 2016 (see 23rd Activity Report, Section 1.6.4). We have discussed with the project managers measures to prevent unauthorised internal access. Whilst each access is logged as a matter of course, ideally there should be automated alerts if, for example, an employee accesses data an unusually large number of times. To protect employees' privacy, a solution involving pseudonymised user data will now be implemented which allows analysis of each access by name if there is a concrete suspicion of an abuse.

The BAGSAN project is also the subject of ongoing political debate. Councillor of States Joachim Eder has put forward a parliamentary initiative calling for the FOPH to only receive grouped data from insurers which, for data protection, cannot be traced back to individual persons. The Federal Act on the Oversight of Social Health Insurance (HIOA) would then be adapted accordingly. Meanwhile, the specially-formed parliamentary sub-committee on "Data delivery" has addressed this issue and written a draft revision for review by the Social Security and Health Committee (SSHC). The SSHC has submitted the preliminary draft, with explanatory report, to the consultation proceedings. If the FOPH were to only receive grouped data from health insurers, this would not render the BAGSAN project obsolete and yet substantial changes would have to be made to it. The FDPIC will continue to closely monitor the BAGSAN project.

Electronic patient record gives rise to new tasks

Work implementing the Electronic Patient Record is progressing apace. From spring 2020, it should be available in all regions of Switzerland. This will create some important new supervisory tasks for the FDPIC. The Confederation and the cantons are pressing ahead with the Electronic Patient Record (EPR), as introduced by the Federal Act on the Electronic Patient Record (EPRA). For it to be available to the general public in all regions of Switzerland from spring 2020, the EPRA requires certified private sector providers to be established, known as communities ("Gemeinschaften") and reference communities ("Stammgemeinschaften"). Data processing activity by these providers will be supplementary to the special provisions of the FADP, the application of which is supervised by our authority. The collectives are private legal entities subject to oversight by the Confederation (regardless of whether the individual members of the collectives are hospitals under public cantonal law or federal private law). Moreover, key components that are necessary to run the EPR system will be operated by the Confederation.

In order to access the EPR, patients and treatment providers alike require means of identification which enable unequivocal authentication. The system will rely on the use of electronic identities, which can be stored on a chip card or a smartphone, for instance. Issuers of EPRA-compliant means of identification must be certified. Data processing in connection with the creation and management of electronic identities is also governed by the FADP. Given the legal and technical requirements that apply to data protection, high standards must be met if patients are to trust the EPR. There-

fore, the FDPIC has been asked by members of parliament to attend various committees of the federal parliament to explain its EPR-re-

lated tasks which, because of the budget constraints imposed by the Federal Council, it must perform without additional staffing. "Helsana+" bonus programme on trial: the FDPIC calls upon the Federal Administrative Court

During the current reporting year, the FDPIC has been taking a closer look at the "Helsana+" bonus programme.

Having issued a recommendation to Helsana Zusatzversicherungen AG, which the company rejected, the FDPIC brought the matter before the Federal Administrative Court.

In the previous reporting period, the FDPIC had already turned its attention to a number of health apps and bonus programmes offered by health insurers, including the "Helsana+" bonus programme run by the Helsana health insurance fund, which was launched in September 2017. This is a scheme designed to encourage participating policyholders to adopt health-conscious behaviour and an active lifestyle. As a reward for their recorded activities, participants receive so-called "Plus Points", which they can convert to cash payments or redeem for offers and discounts at partner companies of Helsana. Unlike similar products offered by other health insurance funds, "Helsana+" is also open to people who have only taken out basic insurance with Helsana.

Having conducted and completed a formal fact-finding procedure at Helsana during the last reporting year, on 26 April 2018 the FDPIC issued a recommendation pursuant to Art. 29 FADP to Helsana Zusatzversicherungen AG. In it, the FDPIC firstly recommended stopping the flow of data from basic to top-up insurance during the registration process, i.e. not processing personal data of basic insurance policyholders during registration for the bonus programme. Secondly, the FDPIC demanded that Helsana Zusatzversicherungen AG refrain from processing the data of customers who only have basic insurance with Helsana, for the purposes of calculating and paying near-cash refunds. The FDPIC takes the view that, commercially speaking, the contested data processing actions are tantamount to ex post reimbursement of a portion of the basic insurance premium, for which there are no provisions in the

As Helsana Zusatzversicherungen AG dismissed its recommendation, the FDPIC decided to present the case to the Federal Administrative Court and brought an action on 18 June 2018.

Data protection Data protection

Data procurement was illegal due to lack of legally valid consent

In a decision dated 19 March 2019, the Federal Administrative Court partly upheld the FDPIC's action. In the absence of legally binding consent,



44

data procurement by the compulsory health insurance provider was unlawful. On the other hand, the additional data processing by

Helsana+ was regarded as lawful. The Federal Administrative Court expressed its fundamental views for the first time on the issue of when data processing carried out for an illegal purpose breaches the Data Protection Act (FADP). The court concluded that data processing for an illegal purpose is only unlawful under the FADP if it contravenes a provision that at least serves to protect personal privacy.

By way of a legal comparison, the court also cited the European General Data Protection Regulation, which goes further than the FADP and the draft for a complete revision of the FADP in only allowing data to be gathered for 'legitimate purposes'.

The Federal Administrative Court aims to restrain on the FDPIC to some extent on its dynamic interpretation of the 1992 FADP with regard to digital applications, thus revealing the limits of this ageing piece of legislation. Because the provisions of the Health Insurance Act that are at issue in the present case do not also serve to protect personal privacy, the Federal Administrative Court was ultimately able leave the question of whether the data processing conforms to the Health Insurance Act open. On this occasion, however, the Court nevertheless held that there was no apparent violation of the Health Insurance Act and thus indicated that it would not agree with the FDPIC's interpretation of the economic implications.

Risks inherent in the rapid proliferation of "personalised health" data

Progressive digitisation in medicine and research is resulting in ever greater volumes of increasingly detailed health data. Data protection principles are paramount, particularly if the data can be traced back to individuals.

The health sector is gathering more and more data, including clinical data from hospitals, surgeries or biobanks as well as data gathered from data subjects themselves. The latter data are obtained by various means, including use of health apps, fitness trackers or medical devices such as blood glucose monitors. "Personalised health" describes the use of these data to develop overall health strategies, identify particular health risks at an earlier stage or develop medical treatments specially tailored to individual patients or patient groups. The growing volume of data is a source of opportunities, challenges and data protection risks for medical research and treatment institutions. To start with, there is the challenge of ensuring the consistent quality and reliability of such data, and their comparability. Technical security or (frequently unforeseen) changes in the purpose of processing are two sources of data protection risks. On top of this, there are a number of ethical questions to be considered. As a united response to these concerns, the "Swiss Personalized Health Network" (SPHN) was launched under the auspices of the Swiss Academy of Medical Sciences (SAMS).

The SPHN has been tasked by the Confederation with creating the foundations and infrastructures to enable research institutions to share healthrelated data and the FDPIC was involved in this work. When processing non-anonymised health data, it is important to ensure transparency at all times with regard to both the



purpose of processing and ←O→ the use of the data concerned, and to obtain patients' legal consent beforehand.

1.6 Employment

Outsourcing: processing of personal data abroad

Many employers decide, for costrelated or organisational reasons, to have their employees' personal data processed abroad. Whilst it is vital that employees are transparently and comprehensively informed about this, their consent is not normally required and would not, in fact, have any validity. Driven by the desire for rationalisation and centralisation, businesses remain very keen to store and process personal data abroad. Over the last reporting year, numerous employees affected by this, as well as employers and HR managers, asked the FDPIC questions about the permissibility and possible permutations of outsourcing. Data are deemed to have been transferred abroad as soon as they are made accessible to a company or entity based abroad or the data are stored in a cloud located abroad. The majority of the questions concerned the duty to inform and obtain the consent of employees when personal data are to be processed in another country. The FDPIC recommends that employers share extensive information with employees about both the transfer of data abroad and the ways in which data

are actually processed abroad, and for what purpose. This includes providing information about the country and company

to which data are exported, how the data are evaluated, and to what end.

This information should not be confused with consent. Since, due to the subordinate nature of the employment relationship, the requirement for consent to be given "voluntarily" (Art. 4 para. 5 FADP) is often not met, usually the employee's consent proves devoid of any legal effect or is unsuitable as justification pursuant to Art. 13 para. 1 FADP. However, at global companies in particular, it seems to be standard practice to obtain employees' consent under data protection guidelines which, under Swiss data protection law, generally prove ineffective. It is up to the competent civil court to determine whether data transmission takes place lawfully in a specific case and the data subjects were adequately informed.

Online application procedures and interviews: the key aspects to consider

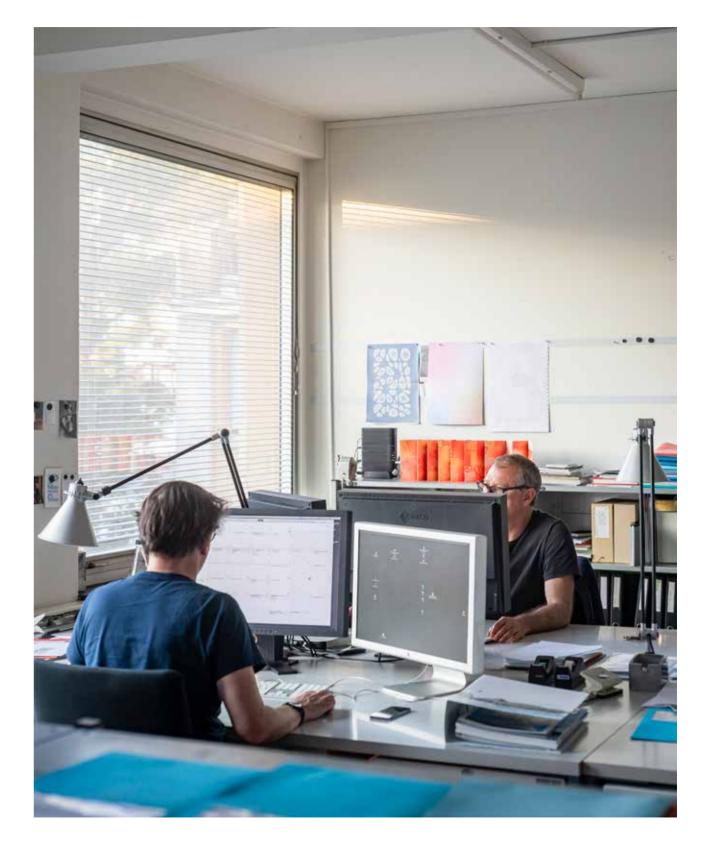
In the digitised work environment, automated behaviour and voice analyses are widely used in the online application process. Since these can be used to produce detailed personality profiles, an increased level of data protection must be assured.

It is becoming increasingly common for job interviews to be conducted online. Both applicants and recruiters are questioning the reliability of, and legal requirements for behaviour and voice analyses. According to Art. 328b CO, in the application process the employer is permitted to process such information about applicants as is necessary to clarify suitability for the role or perform the employment contract. In its advisory capacity, the FDPIC has pointed out that the processing of CVs and other information by HR managers frequently involves the processing of essential characteristics of the applicant's personality or of personality profiles within the mean-



ing of Art. 3(d) FADP. This is particularly true when behaviour or voice analyses are carried out on recordings of job inter-

views. The analyses must be proportionate and suitable data security measures must be taken. Applicants must be informed beforehand not only about the planned analyses, but also about the manner in which, and purpose for which the results will be used, how long they will be kept and the applicant's right to obtain information.



Data protection Data protection

Combating illegal employment in the canton of Valais

At the intervention of the FDPIC, the ARCC association shut down its epony mous smartphone app. This had been used for more rigorous monitoring of construction sites in Valais. The FDPIC is demanding that the data already obtained via the app be erased.

A number of joint committees in the canton of Valais formed the ARCC association (in French: Association pour le Renforcement des Contrôles sur les Chantiers, ARCC) for closer supervision of construction sites. The association is mainly concerned with monitoring compliance with the ban on illegal employment and the Posted Workers Act. Based on comments received, we carried out an investigation at the association in accordance with Art. 29 FADP. The focus of the FDPIC investigation was the smartphone application "ARCC", which allows reports to be sent directly to the association.

The app is used to send photos which show the name of the construction company concerned and, in some cases, even construction site workers. as well as information about the name and location of the person using the app. In the course of our investigations, the association shut down the app. The FDPIC takes the view that, at present, there is no adequate legal basis for operating the app or for the data processing actions resulting from its use. We therefore welcome its deactivation and have made a written request to the association to destroy the personal data already collected. Furthermore, we have made the association aware that it runs the risk of potential civil suits by data subjects, should it continue processing the collected data.

1.7 Insurance

New observation article for social insurance

Covert observations are an effective tool in exposing fraud and abuses of the social insurance system. As such measures are a massive invasion of privacy, they must be kept to the bare and necessary minimum. The FDPIC welcomes the requirement of authorisation for the use of technical devices for location tracking.

In a referendum held on 25 November 2018, voters approved the new observation article regarding covert surveillance for social insurance purposes. The new provision is likely to enter into force in the autumn of 2019. At the appropriate time, we will use the opportunity to comment on the implementing provisions that will be incorporated in an ordinance. The requirements to be met by the external specialists who will be tasked with observation are particularly relevant



from a data protection perspective. Guarantees which guard as far as possible against the misuse of observation mate-

rial must be incorporated in the selection process. This might also entail an approval process.

The FDPIC also expects clarification of certain aspects by ordinance, or would at least expect directives on observing insured persons whose location can be seen from a freely accessible location.



In line with the principle of proportionality, private areas such as the interior of a residence must be protected within the meaning of set-

tled case-law of the Federal Supreme Court. We welcome the fact that a court approval must be obtained for the use of technical tracking instruments. Such approval may only be granted if the court is satisfied of the genuine need to use such devices in the specific case in question. Therefore, no tracking devices may be used, on vehicles for instance, without the court's authorisation. Video and audio recordings can, however, still be made without obtaining judicial authorisation.

The Commissioner also considers it an obligation – enshrined in the new observation article - to subsequently inform the insured person if observation has failed to confirm the suspected abuse. In this case, the insurer must issue a decision detailing the reason, nature and duration of the observation. Insured persons can demand to see the observation mate-



rial and then decide whether the material can be kept on file or is to be destroyed. However, the insurer cannot destroy the observation

material until the decision has become final, and may only do so if the insured person has not explicitly stated that the material is to be kept on file.

SUVA: more transparency in research using insured persons' data

In partnership with the FDPIC, SUVA has greatly improved the information pro-



vided to insured persons regarding the use of their data for research purposes. Interested parties will find important infor-

mation about the use of insured persons' data for research purposes, and the right to object, on SUVA's website.

SUVA uses insured persons' data for research purposes (usually in cooperation with third parties) in the area of insurance and rehabilitative medicine. In our advisory capacity, we have ensured that SUVA provides detailed information on its website (in the section headed Accidents - Medical Research) about why and in what areas it uses insured persons' data for research purposes. SUVA's research activity focuses predominantly on the musculoskeletal system, occupational diseases, traumatic brain injuries, chronic pain, the psychological impact of accidents, and amputation. However, the research also serves to improve assessment methods and prevention. Now, SUVA provides clear information about the fact that each insured person has a right to object and how that right can easily be exercised.

By publishing the relevant information on its website, SUVA can continue making a valuable contribution to medical research. At the same time, it is upholding the data protection principle of perceptibility and transparency of data processing. Participation in research projects and making personal data available for research projects remain voluntary for insured persons and must not influence medical care or the assessment of a claim. Treating specialists also have an important role to play, in informing patients that they have a right to veto



the use of their data for research purposes. If the patient notifies SUVA that s/he does not wish his/her data to be used for research

purposes, SUVA adds a note to the file to prevent such use.

As part of the same project, our advice also resulted in SUVA reviewing and, where necessary, adapting its internal guidelines. We stressed the need for personal data to be anonymised at the earliest possible stage. Moreover, when working with non-anonymised or non-pseudonymised data, the researchers must conclude specific confidentiality agreements with SUVA. When using anonymised or pseudonymised data, they are not permitted to process data in a manner which could enable the re-identification of individuals. In particular, the research data must not be linked with data from other sources. Furthermore, once the research project is complete and the results have been published, the data must be erased. Researchers must confirm this to SUVA, in writing. Information about this is now available for researchers on SUVA's website. Whilst our consultation process is now over, it is up to SUVA to make sure that the information and internal guidelines always satisfy the requirements of the data protection act, including when new treatment and research methods are used. The handling of genetic material or results of genetic tests (in such spheres as highly specialised medicine) merits particular attention.

1.8 Traffic

Multimodal mobility -Safeguards of informational self-determination are essential

The DETEC has been commissioned by the Federal Council to investigate ways of promoting multimodal mobility and exploiting its potential. The objective is to offer passengers a simple, flexible combination of various mobility offers on all traffic channels. The FDPIC oversaw the project during the reporting year, advised providers on data protection matters and expressed his opinion during the office consultation.

New digital technologies are to be used to make it easier for passengers to find out information about combinations of different mobility offers. This involves processing large quantities of personal data. The FDPIC monitored the project, which is still in the initial stage, and advised the providers of multimodal mobility services on various occasions, including at a number of meetings. Providers are aware that, when processing personal data, it is



essential to safeguard data subjects' informational self-determination and that specific measures must be taken to protect data sub-

jects' personal rights. The FDPIC pointed out that, in particular, users must not be compelled – whether directly or indirectly – to disclose personal data. To ensure that data subjects give consent freely, they must first be transparently informed about the type of data processing to which they are consenting by selecting a particular mobility service, and about the alternative choice available to them. If linkage of factual data not covered by the

data protection act enables individuals to be identified, the data protection provisions must be satisfied.

The FDPIC also drew attention to the ease with which movement profiles can be obtained from use of multimodal mobility services in order to then derive personality profiles. In this case, the increased level of protection for sensitive personal data and personality profiles must be assured.

Real choice and anonymous travel for customers

During the official consultation, the FDPIC also gave an opinion on multimodal mobility. He commented on the planned revision of the provision in the Passenger Transport Act concerning data processing by public transport companies. The purpose of this revision is to make public transport companies subject, when processing data, to the data protection regulations for private individuals rather than those applicable to federal bodies. This would mean that, with the passengers' consent, they can process passengers' data for certain purposes. The FDPIC did not agree with the proposed wording, pointing out that, in this instance, customer consent could only be deemed valid if freely given, i.e. if based on real choice. In the case of automatic ticketing, this would mean that – as an alternative to the planned models - customers must also have the option of travelling anonymously, subject to the same conditions (i.e. without suffering any discrimination). Furthermore, the FDPIC said, there must still be a legal basis for the processing of personal data for the purposes of executive administration. The FDPIC welcomes the inclusion of his comments in the consultation draft.

The FDPIC will continue monitoring the project. In due course, the data protection risks associated with the project must be evaluated.

Data protection Data protection

Privacy compliance of new public transport apps

The transport sector has informed us about various projects, including the continued development of various apps. Privacy compliance must constantly be reassessed. In particular, only the data necessary for the provision of a service may be collected.

This year, the FDPIC was again notified of data protection projects by a few transport companies. These included data processing actions in connection with the continued development of a number of apps operated by transport companies, in particular Swiss Federal Railways (SBB). In some instances, anonymised data were involved, although data subjects are nonetheless identifiable. In such cases. the term 'anonymised data' may not be used in the information provided to data subjects. The FDPIC made the transport company aware that it must meticulously re-examine the issue of anonymisation before undertaking any further data processing. To the same



end, the FDPIC made SBB aware that the principles of proportionality and data minimisation must be observed when processing

data. This is also the case if consent was obtained for the data processing. It is important that transport companies safeguard privacy compliance in each project. Both planned and previous data processing operations must be checked and, if necessary, brought into line with the requirements of data protection law. Privacy compliance must be re-analysed each time apps are



1.9 International

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 gave their view on the EU Commission's proposals for interoperability between the EU information

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 12/13 June 2018 and 14/15 November 2018, in Brussels. The European Data Protection Supervisor (EDPS) and the national data protection authorities of the 28 EU member states were represented, with Ireland and the UK attending as observers. The groups were supplemented by the national data protection authorities of Switzerland, Liechtenstein, Norway and Iceland, as their countries participate in the information systems.

The SIS and Eurodac Supervision Coordination Groups also adopted their 2016/2017 activity reports. In a document for submission to the EU Parliament, the EU Council and the EU Commission, they commented on the EU Commission's proposals for a regulation which will establish the framework for interoperability between EU information systems. Meanwhile, the VIS group prepared and sent an opinion to those committees on the changes to the VIS proposed by the EU Commission (see also www.sis2scg.eu, www.visscg.eu, www.eurodacscg.eu).

Currently the secretary of the three Supervision Coordination Groups is managed by the European Data Protection Supervisor. In future, their management will be transferred to the European Data Protection Board (EDPB).

Sub-Working Group on "Border, Travel & Law Enforcement"

During the year under review, as a Schengen member country the FDPIC attended seven meetings of the sub-working group, chiefly to discuss the interoperability of large-scale IT systems in the European Union in the areas of migration, asylum and security, as well as the future of models for monitoring large-scale IT systems in the EU in the area of justice and internal policies.

One of the major topics of discussion at these meetings was the interoperability of large-scale IT systems in the European Union (both current and future) in the areas of migration, asvlum and security. In December 2017. the Commission published two proposals for regulations on the establishment of a legal framework for the interoperability of large-scale EU information systems. This new approach and the new components introduced (creation of a European search portal, a shared biometric matching service and a common identity repository) have repercussions not only for data protection, but also the governance and monitoring of systems. A number of concerns were raised from a data protection perspective, such as the purposes of a centralised database, and the conditions and terms of its use. Both the European Data Protection Supervisor and the national data protection authorities are calling for real guarantees to protect the fundamental rights of third-country nationals (for more on this, see the opinion of the European

Data Protection Supervisor dated 16 April 2018, via the following link edps.europa.eu/data-protection).

The future of models for monitoring the EU's large-scale information systems in the area of justice and the police was also discussed at the various meetings. The idea is to find an option permitting improvements to the mechanism by which these various systems are monitored, for instance by transferring monitoring to a new structure attached to the European Data Protection Board (the successor to the "Article 29" working party, made up of the European Data Protection Supervisor and the national data protection authorities), membership of which could also be open to non-member states with observer status for issues relating to the Schengen acquis.

Moreover, guidelines are currently being drawn up in relation to the EU Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Directive EU 2016/680) and, in particular, in relation to Article 47 and the powers of the supervisory authorities.

54

Swiss Data Protection Authorities Coordination Group for the Implementation of the Schengen Association Agreement

The Swiss Data Protection Authorities Coordination Group for the Implementation of the Schengen Association Agreement met twice during the year under review. The FDPIC informed the cantonal data protection authorities of the main points discussed during the Schengen evaluation and the recommendations made by the EU Council. In Switzerland, Schengen-related activities are coordinated by the "Swiss Data Protection Authorities Coordination Group for the Implementation of the Schengen Association Agreement", which brings together the FDPIC and the cantonal data protection authorities. It is a platform for the authorities represented to find out about the latest Schengenrelated developments, plan supervisory activities and share information. Through this platform, we coordinate with our cantonal counterparts our data processing supervision activities in Switzerland in the area of migration, police and criminal justice, in application of the Schengen agreement.

The Swiss Data Protection Authorities Coordination Group met twice during the year under review. At the first meeting, the FDPIC informed the cantonal data protection authorities about the main points raised during the Schengen evaluation of Switzerland, which took place between 26 February and 2 March 2018 (see above). The cantonal data protection authority evaluated (Lucerne) also gave a summary of the aspects that are of particular relevance both to it and to the other cantonal bodies concerned. We also provided details to our cantonal counterparts of the various SIS/ VIS inspections we carried out during the year under review. The cantons themselves presented the results of their supervision activities.

At the second meeting, the FDPIC elaborated on the recommendations sent to Switzerland regarding the data protection aspect of the Schengen evaluation. We also informed our cantonal colleagues about the main points addressed by the SIS/VIS supervision coordination groups.

International Conference of Data Protection and Privacy Commissioners

The 40th International Conference of Data Protection and Privacy Commissioners focused on the digital revolution and its impact on our societies, and how new digital ethics could help guarantee respect and dignity in our technology-dominated world. A working group on artificial intelligence was formed.

The Conference took place in Brussels, from 22 to 26 October 2018, under the aegis of the European Data Protection Supervisor (EDPS) and the Bulgarian Commission for Personal Data Protection, and its theme was "Debating Ethics: Dignity and respect in a data driven life". As stressed by Isabelle Falque-Pierrotin, President of the CNIL and Chair of the International Conference, in her opening address, these subjects "have taken on a new dimension and encompass new issues of a more political and ethical nature. They are being played out in an international environment which, though never peaceful, is particularly unsettled right now. Whilst there are tensions, including around issues that lie at the heart of what we do, such as data localisation, cyber security, mass surveillance and information techniques (...), the digital realm is also a unique development opportunity on a global scale, a revolution in the true sense. Going forward, "tech for good" or "Al for humanity" will be on the agendas of meetings of our heads of state and government, and these technologies have tremendous potential to offer solutions for humanity.

Declaration on ethics and data protection in artificial intelligence

For the first time, the conference was organised jointly by a European institution and a national data protection authority. It brought together more than 1000 participants, who debated the latest privacy issues. During the closed sessions, the commissioners admitted four new members from national data protection authorities: Argentina's Agency of Access to Public Information, the Bavarian Data Protection Authority, the Lower Saxony data protection authority and the Korea Communications Commission. The Conference currently has 123 members. Elections were held to appoint a new Chair: Elizabeth Denham, Information Commissioner of ICO, who succeeds Isabelle Falque-Pierrotin (President of the CNIL). The next international conference will be held in Tirana from 21 to 25 October 2019.

The closed session adopted a historic text, the Declaration on ethics and data protection in artificial intelligence. The declaration enacts six guiding principles which constitute the fundamental values for the preservation of human rights in the development of artificial intelligence. Finally, the Conference adopted five resolutions on the following: e-learning platforms, the amendment of rules and procedures for the international conference, the roadmap for the future of the international conference, collaboration between data protection authorities and consumer protection, and the resolution on the conference census.

Conference of European Data Protection Authorities

The Conference provided an overall view of the problems surrounding implementation of the GDPR, which provides the 28 current Member States of the European Union with a robust, standard legal framework.

This 28th edition of the conference, entitled "Data Protection - Better Together" was held in Tirana, Albania, on 3 and 4 May 2018. Participants also debated the modernisation of Convention 108 of the Council of Europe, which is aimed in particular at facilitating cooperation between the Parties, the integration of European data protection standards by other regulatory systems and the processing of personal data in humanitarian actions. The European conference decided to extend and clarify the mandate of the Working Group on the future of the conference, of which the FDPIC is part. The Working Group must prepare concrete proposals for the modernisation of the rules and procedures of this forum, which will, in all likelihood, be called upon to play a significant role in collaboration between data protection authorities. Finally, the conference discussed a draft document to promote and reinforce cooperation and the sharing of experiences between the Member States of the EU and third countries within the framework of the GDPR.

OECD Working Party on Security and Privacy in the Digital Economy (SPDE)

The Working Party on Security and Privacy in the Digital Economy (SPDE) of the Organisation for Economic Co-operation and Development (OECD) has concentrated on number of recommendations.

The Working Party has examined the revised version of the draft OECD Recommendation on critical information infrastructure protection (CIIP). The draft highlights the importance of security guidelines for the protection of critical infrastructures and provides guidance on national policies, while also proposing ways of improving international cooperation for the protection of these infrastructures. It identifies the need for greater international cooperation to tackle transnational problems, given the importance of the Internet as a global infrastructure. The delegates discussed ways of improving data for developing security and privacy policies, and in particular at ways of improving the comparability of reports of data breaches. They then discussed the recommendation made in 2012 concerning the protection of children online, which is currently being revised.

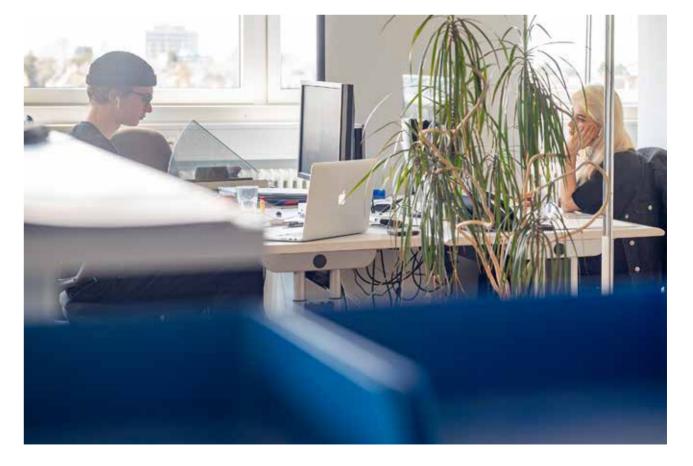
In 2013, the OECD adopted revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which update the original version from 1980. These revised guidelines provide for monitoring of their implementation and a report after five years. Therefore, at its meeting on 13 on 14 November, the working party examined and approved a process for reviewing these guidelines and was mandated to establish an expert group, of which the FDPIC will form part.

The Francophone Association of Data Protection Authorities (AFAPDP)

Among other things, the AFAPDP organised a round table on social networks and electoral processes, involving experts on electoral issues and representatives of political parties.

The Francophone Association of Data Protection Authorities (AFAPDP) held a conference in Paris on 18 and 19 October 2018. The FDPIC has been a contributing member of the association since its creation in 2007. Back then, its members adopted a resolution on the ownership of personal data, in which the association draws attention to the fact that personal data are a constituent element of the individual

person; as such, it is necessary to support the adoption of legislation on the protection of personal data and privacy within the Francophone space, as a prerequisite for upholding democracy and the rule of law in our societies. Such legislation must enable individuals to fully exercise the inalienable rights attached to their personal data by assuring them of a high degree of control over those data. Finally, the AFAPDP proposed a meeting for the various authorities to share their experiences, five months after the GDPR entered into force.



Focus III

The GDPR - also applicable in Switzerland in some instances

The new European General Data Protection Regulation (GDPR) entered into force in the European Union on 25 May 2018. In some circumstances, it also applies to the processing of data by Swiss companies. The FDPIC has published a Code of Practice and attended numerous information sessions as part of his advisory and awareness-raising role.

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 EU: 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. The new rules give persons in the territory of the European Union greater control over their personal data, place greater responsibility on companies while reducing their reporting burden and reinforce the role of the data protection authorities.

One of the biggest initial difficulties faced by a data protection authority in a third country such as Switzerland lies in the vague nature of the concepts of "offering goods and services to persons located in the territory of the European Union" and of "monitoring the behaviour of such persons". Second-guessing and identifying the boundaries of a text which we did not write and is not ours to interpret is a hazardous exercise. However, as Switzerland is also directly impacted by this new legal instrument, the FDPIC has published a Code of Practice which, in particular, tackles the extraterritorial application of the new European law. In essence, the extent to which the Regulation applies must always be assessed on a case-by-case basis, considering in particular the controller's intention to offer goods or services to persons located in the territory of the European Union or to monitor their behaviour.

Guidelines on the scope of application of the GDPR

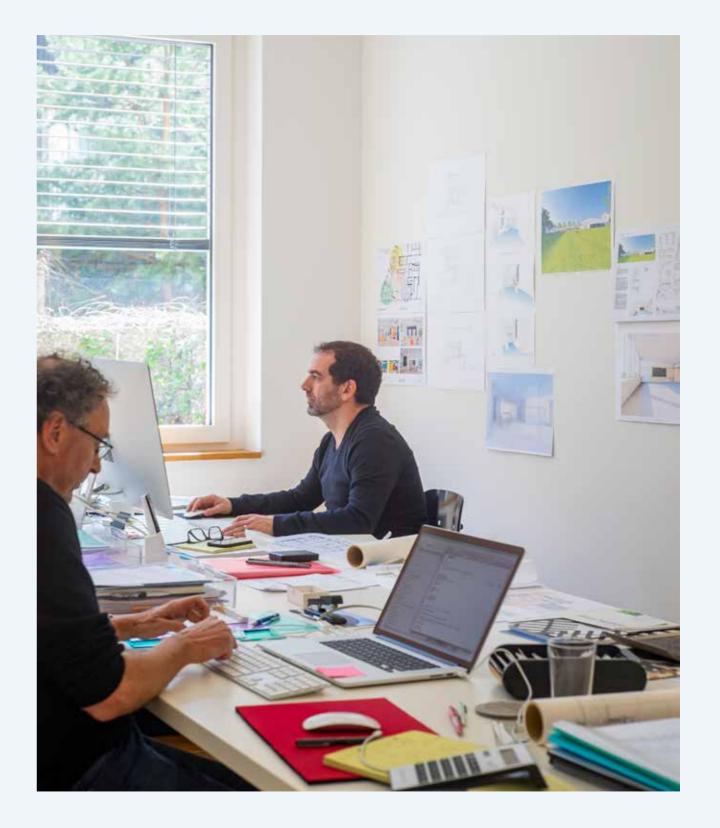
The FDPIC has spoken at numerous information sessions held on this subject by the federal administration and by private sector bodies. In his advisory role, he has also answered a great many oral and written questions from the general population and the media.

As the European French-speaking authorities which are not members of the EU are faced with the same difficulties, they have gathered several times over the course of the year to share their experiences and pool the questions put to them, in order to coordinate their responses

More than six months after the GDPR entered into force, the European Data Protection Board (EPDB) – 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. A public consultation was held to discuss these guidelines, attended by the FDPIC in collaboration with the Monegasque authorities (CCIN), to seek clarification on a number of aspects of this extremely important issue for third countries that are part of the EU landscape.

Evaluation of data protection level

The European Commission is investigating the level of data protection in third countries and last stated that it considers the level of data protection in Switzerland appropriated in 2000. Companies in the EU can therefore exchange personal data with companies in Switzerland without taking further measures. The European Commission is currently re-evaluating whether the level of data protection in Switzerland is appropriate according to the criteria listed in the GDPR. It has announced that it will publish a report setting out its decision on this issue in May 2020. Swiss participation in the evaluation is being coordinated by the Federal Office of Justice and the FDPIC is providing support by making the requested information available (see Chapter IV).



Focus III

Council of Europe - Switzerland should ratify the adapted Convention as soon as practicable

Convention 108 has been modernised and opened for signature. Thus far, 22 States have signed it. Unfortunately, Switzerland, which played a leading role throughout the development and adoption phase, is not among the signatory states, preferring to wait and see how the revision of the FADP progresses.

Efforts to modernise the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) culminated on 18 May 2018, when a Protocol of Amendment (STCE 223) was adopted by the Committee of Ministers of the Council of Europe. The modernised Convention (Convention 108+) was opened for signature by the Parties on 10 October 2018.

Convention 108+ reaffirms the basic principles of data protection. It reinforces a number of principles such as the principle of proportionality, clarifies the conditions for lawfulness of processing of personal data. Furthermore the Convention 108+ introduces new guarantees and rights for data subjects, such as the right not to be subject to automated decision-making, the right to obtain knowledge of the motives for data processing, the right to object and the right to benefit from the assistance of a supervisory authority.

It also introduces duties for data controllers, such as notifying data breaches, ensuring compliance, risk assessments, designing processing steps in a manner which prevents or minimises the risks of infringements of fundamental rights and freedoms, and transparency obligations. It regulates the international transfer of data, and it specifies and widens the competencies and powers of supervisory authorities and their duties to cooperate. It establishes a mechanism for monitoring and evaluating observance of the provisions of the Convention.

A necessary modernisation which takes account of the global and digital reality

The modernisation was necessary to accommodate technological and legal developments since 1981. It is intended as a credible and effective response to the current reality of the globalised, digital world.

The Convention is a binding international instrument. Its universal, all-encompassing nature has been taken into account in the modernised version, which is worded in general, simple terms, without any technological references. Today, there are 53 parties to the Convention (47 member states of the Council of Europe and 6 third countries: Cape Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay). Three other States have been invited to join and eleven others have observer status on the consultative committee.

Brexit and transfer of the personal data

Following the referendum held in June 2016 in the United Kingdom on leaving the EU (Brexit), the British Government informed the Union of its decision to resign. The United Kingdom's withdrawal should have been taken place on 29 March 2019 but it has been postponed to a later date.

The FDPIC has been involved in numerous meetings with the federal and UK authorities in order to ensure that free movement of personal data between Switzerland and the United Kingdom remains possible after the latter is no longer an EU member state. The United Kingdom has currently an adequate level of data protection and the FDPIC has no reason at present to believe that the United Kingdom's status will change.

Convention 108+ is regarded as the benchmark for an adequate level of data protection

The Protocol of modification will enter into force when all the Parties have agreed to it, or if 38 Parties have agreed to it in a five-year period. When the text was adopted, the Committee of Ministers urged all the Parties to do their utmost to ensure its swift entry into force. The ratification of Convention 108+ is an essential criterion for the European Union to uphold the validity of its decision to recognise the adequate level of data protection of a third country. This is particularly crucial for the economic and financial centres of third countries such as Switzerland, because the free movement of data between Switzerland and the EU depends on it.

Not least in regard of the ongoing evaluation by the European Commission (see point III above), it is in the interest of Switzerland to sign the protocol of modification as soon as possible and subsequently ratify it. This implies that the revision of the Federal Act on Data Protection pending before the Federal Parliament is carried out in accordance with the provisions of Convention 108+, as proposed by the Federal Council in its presented revision in September 2017. The cantons must adapt their legislation in a timely manner, too.

The Consultative Committee of Convention 108 (T-PD) has adopted a draft recommendation on the protection of health-related data. This recommendation, which should be adopted by the Committee of Ministers sometime this year, replaces recommendation R (97) 5 on the protection of medical data. It accommodates technological advances since 1997 and Convention 108+. The T-PD has also adopted a practical guide on the protection of data in the police sector, which is aimed primarily at the police forces and illustrates the principles and rules of data protection. In addition, it has adopted guidelines on safeguarding privacy in the media, drawn up jointly with the Steering Committee on Media and Information Society (CDMSI), and a Guide on privacy and data protection principles for ICANN related data processing (Internet Corporation for Assigned Names and Numbers). Finally, the T-PD is working on guidelines for data protection and artificial intelligence, as well as on evaluation and follow-up mechanisms for Convention 108+.

2.1 Generally

The consolidation of the paradigm shift towards an open and transparent administration, which is the aim of introducing the principle of freedom of information, is making steady progress: The implementation of the Freedom of Information Act by the federal authorities can generally be regarded as a positive move. This is also shown by the fact that the number of requests for access that are granted in full is keeping pace with the increasing overall number of applications, and that the percentage of requests for access that are refused outright has decreased steadily over the years (see Section 2.2).

It is equally pleasing to see that the Freedom of Information Act is having a positive influence on the federal authorities' active information policy: in response to requests for access and for mediation, ENSI is now publishing details of the emission values measured at Swiss nuclear power plants every month (ANPA-EMI-data) and the SFOE publishes the results of the implementation of the CO₂ emission regulations on passenger cars each year. In order to promote transparency, armasuisse publishes a register of offset transactions, while the DDPS's internal audit department publishes its audit reports.

Thanks to the introduction of an accelerated conciliation procedure following a successful pilot project, positive results were again achieved in the year under review in terms of processing time and the number of settlements achieved (see Section 2.2).

Proceedings involving three or

more parties have proved challenging for all concerned. These include proceedings relating to reports on administrative or disciplinary investigations, and documents with possible trade secrets or that relate to protecting the privacy of private individuals or government employees. These mediation proceedings often involve complex clarification procedures with the third parties concerned. This is not least due to the growing tendency for third parties to call in lawyers at the access and mediation procedure stages. This overly legalistic approach to these - informal - steps in the procedure leads to delays in applicants being granted access. This trend is clearly contrary to parliament's intention to provide simple and quick access and mediation procedures. Where legal questions have to be answered, ordinary administrative procedure should apply, i.e. the authority issues a ruling which can then be challenged before the Federal Administrative Court.

2.2 Requests for access - Constant growth

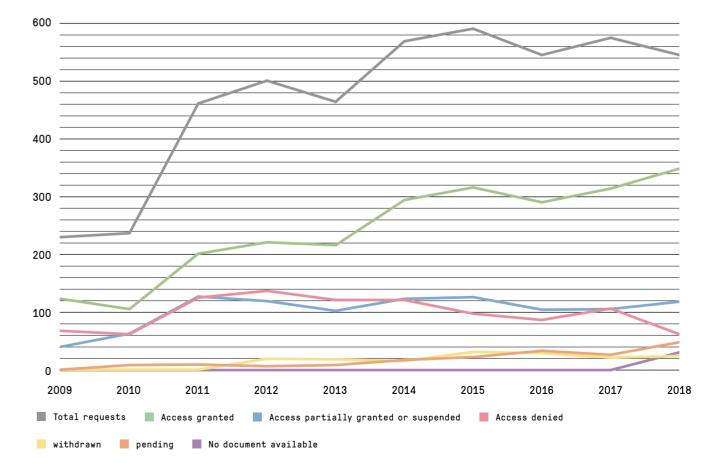
According to figures provided to us for 2018, 636 requests for access were submitted to the federal authorities (compared with 581 in 2017). This equates to an increase of 9.5 percent. Including the Public Prosecutor of the Swiss Confederation (8) and the Parliamentary Services (3), the complete is 647.

The authorities granted full access in 352 cases, which is 55 percent of the complete (compared with 317 in 2017, or 55 percent of the complete). In 119 cases (19 percent), applicants were only granted partial access to the documents (compared with 106 in 2017, or 18 percent). Access was completely denied in 62 cases (ten percent) compared with 107, or 18 percent, in

2017. Furthermore, the authorities announced that 24 requests for access (four percent) were withdrawn (compared with 21 in 2017, or four percent), 48 requests (eight percent) were still pending at the end of 2018 (compared with 26 in 2017 or five percent) and in 31 cases (five percent), there was no official document.

Overall, the Commissioner notes that, following a sharp upturn in the number of requests for access in 2011, the figure has continued to grow steadily. However, the increase was even bigger in 2018 than the previous year, with the number of requests exceeding 600 for the first time. Figures relating to the authorities' handling of requests for access are generally stable com-

pared with previous years. The Commissioner notes that, since 2015, the number of requests leading to full access being granted has stabilised at over fifty percent. In comparison, the number of requests for access that are denied outright has steadily fallen since 2015. The new statistical distinction, introduced in 2018, between denial of access and absence of official documents may be one of the factors behind this drop.



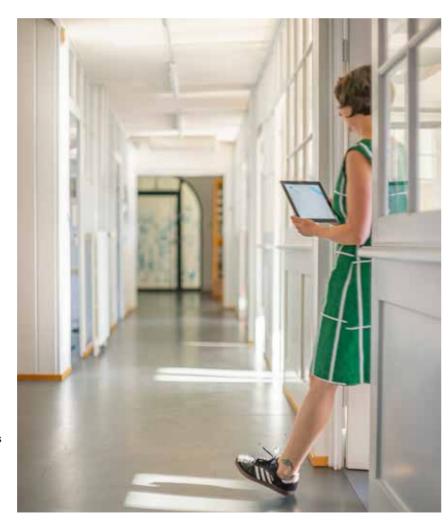
Federal departments and agencies

With regard to the figures notified to the Commissioner by the agencies, the Commissioner notes that the FOPH received the most requests for access in 2018 (42), followed by the FOT (27) and Swissmedic (24). The departments which received the most requests are the FDFA (156) and the FDHA (112). Conversely, 16 authorities informed us that no requests for access were submitted to them during 2018. Over that same period, the Commissioner himself received seven requests. He granted full access in four cases, partial access in one, another case is still pending and, for the remaining case, the requested document did not exist.

In 2018, just 17 requests for access incurred a fee, i.e. 2.62 percent (compared with 1.89 percent in 2017). Just nine authorities charged fees. Fees received for access to documents complete 13 358 Swiss francs. Although this is a higher complete than in 2017 (CHF 6160), it is still not out of the ordinary compared with previous years (2016: CHF 22 700, 2015: CHF 13 663). As in previous years, fee-charging was the exception, as access was granted free of charge in nearly 98 percent of cases. Whereas the Federal Chancellery, the FDJP, the FDFA and the FDF did not charge any fees, the other four departments did, in a minority of cases, invoice the applicants for the time spent dealing with their request. The FDHA (CHF 10 900 for eight requests) and the DETEC (CHF 1300 for three requests) accounted for the bulk of fees charged.

As regards accounting for 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. Details are provided to the Commissioner on a purely voluntary basis and only partially reflect the working hours actually devoted to handling requests. According to these data, the working hours published this year increased by 63 percent compared with the previous year (2018: 4827 hours; 2017: 2968 hours).

This increase correlates with a greater number of requests for access than in previous years. Time spent preparing for mediation sessions decreased significantly compared with previous years (2018: 672 hours; 2017: 914 hours; 2016: 857 hours). In many cases, time spent on issuing a ruling or on appeal proceedings was not accounted for, or notified to the Commissioner.



Parliamentary Services

The Parliamentary Services informed us that they received three requests for access in 2018. Access was denied outright in two cases and there were no official documents for the other case.

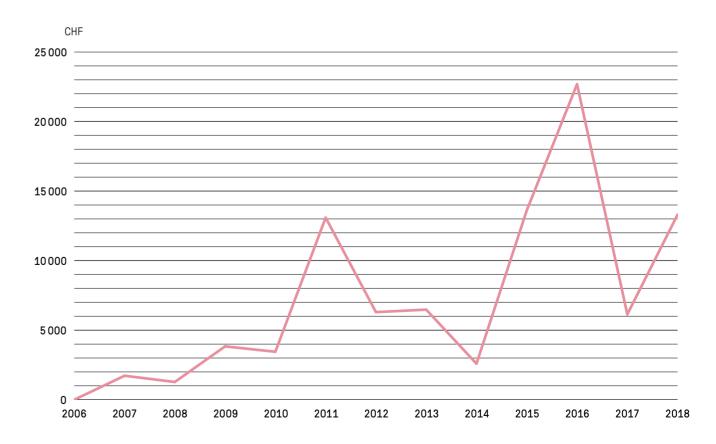
The Public Prosecutor of the Swiss Confederation

The Public Prosecutor of the Swiss Confederation notified us that he received eight requests and that full access was granted three times and denied outright twice. As for the remaining cases, two requests are still pending and, in one case, there were no official documents.

Mediation requests

In 2018, 76 mediation requests were filed with the Commissioner, which is three cases fewer than in 2017 (79). In contrast to previous years, private individuals (26) and the media (24) filed a similar number of requests. From these figures, we can deduce that, in 212 cases, the Federal Administration completely denied access (62) or partially denied access (119) or was unable to grant access as there were no documents (31).

These data must also be considered in the light of the 76 mediation requests received by the Commissioner. During the year under review, mediation requests were submitted for 36 percent of these unmet requests for access (compared with 37 percent in 2017).



2.3 Mediation procedure

As mentioned in the previous activity report, a pilot project was conducted in 2017 with the aim of speeding up mediation procedures. For the pilot project, most of the requests were dealt with at oral mediation sessions, attended by the people and authorities concerned. If no agreement was reached at the mediation sessions, a written recommendation with a summary statement of reasons was sent to the parties. Given the success of the measures taken, the new method has been incorporated in the routine management of procedures. The data collected in 2018 are shown below for comparison and evaluation purposes. Therefore, the chapter structure reflects the three objectives of the 2017 pilot project, which are:

- Time taken to process mediation procedures;
- Increase in proportion of amicable outcomes;
- Medium-term reduction in pending cases

Processing time

In Table 1, mediation procedures have first been assigned to one of the following categories, depending on how long it took to settle them: statutory thirty-day period observed, processing time of between 31 and 99 days, processing time in excess of one hundred days. The average time taken to process mediation requests between 2014 and 2016 and in 2017 and 2018 was then incorporated as a percentage in the various aforementioned categories.

Thanks to the pilot project, the length of time has been reduced and this trend was confirmed by the data collected for 2018. The thirty-day period was met in 32 out of 64 mediation procedures, which equates to fifty percent of the requests heard. Moreover, no case took longer than one hundred days to process.

In many cases, failure to meet the thirtv-day deadline was 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. It should be added that the abovementioned situations frequently entail a substantially higher workload and, in such cases, in accordance with Article 12a of the Freedom of Information Ordinance (FoIO; RS 152.310, the Commissioner may extend the deadline by a reasonable period. Nonetheless, the Commissioner notes that the percentage of cases handled within a thirty-day period remains stable compared with 2017.

Table 1: Processing time of mediation procedures

Processing time in days	Period 2014 - August 2016°	Pilot period 2017	Period 2018
within a delay of 30 days	11%	59%	50%
within 31 to 99 days	45%	37%	50%
more than 100 days	44%	4 %	0 %

 $[\]ensuremath{^{\circ}}$ Source: presentation by the Commissioner, event marking ten years of LTrans, 2 September 2016

Proportion of amicable outcomes

To measure the effects of incorporating the pilot project in routine management, three periods will be analysed. The first is the period from 2013 to 2016, the second 2017 (the year in which the pilot project was run) and the third and final one is 2018, the first full year in which the results of the pilot project had an impact.

Table 2: Ratio of recommendations to amicable outcomes

2013 - 2016	40%
2017	60%
2018	55%

The Commissioner notes that the increase in the proportion of amicable outcomes compared with recommendations has remained stable and, therefore, the positive effects of the 2017 pilot project continued in 2018. Running the pilot project led to a significant increase in amicable outcomes compared with previous years.

For anyone interested, all the recommendations made during the year under review are available on the Commissioner's website.

Number of pending cases

Table 3: Pending mediation procedures

Fin 2016	33
Fin 2017	3 (of which 2 in progress)
Fin 2018	15 (of which 13 settled in February 2019)

In 2017, following the launch of the pilot project, just three procedures were pending at year-end (compared with 33 in 2016). For 2018, 15 cases were still pending; ten mediation requests were filed in December alone. It should be noted that, in January 2019, five of these procedures were closed and three were suspended. A mediation procedure is suspended when an authority wishes to re-examine its position or has to consult the third parties involved.

Although the number of pending procedures increased compared with the end of 2017, the Commissioner notes that this is not due to a decline in efficiency. Rather it is a statistical coincidence, in that a large number of mediation requests were filed in December. Therefore, there is still a marked downturn in pending cases compared with previous years.

2.4 Office consultations and other commentaries

Complete revision of the Federal Act on Public Procurement

Parliament has debated a comprehensive revision of the Federal Act on Public Procurement. The Federal Council's proposal to abolish the principle of freedom of information in procurement was rejected. The Commissioner voiced his strong opposition to this proposal, both on the relevant committee and in the media.

Calls for tenders and acceptances of bids by the Confederation are published on the procurement platform simap.ch. While the award procedure is ongoing, there is no right to inspect the procurement documents. Pursuant to the Freedom of Information Act, the documents can only be inspected – on request – once the procedure is complete.

Under the Federal Council's draft revision, all documents relating to the procurement procedure would be definitively removed from the scope of application of the Freedom of Information Act and the right of access for citizens abolished, without substitution (see also 24th Activity Report 2016/2017, section 2.3.2).

Parliament debated the bill during 2018 and rejected the proposed special arrangement. As a result, with the exception of sensitive content from a competitive perspective, procurement documents will remain subject to the Freedom of Information Act, meaning they will generally be accessible. Companies, the media and the general public can therefore continue checking how the authorities use taxpavers' money in the procurement of goods and services. Moreover, when parliamentary motion 14.3045 is implemented in the procurement ordinance, this will introduce a rule under which all procurement procedures with a contract volume of CHF 50 000 or more are published at least once a year. Overall, therefore, the revision will increase transparency.

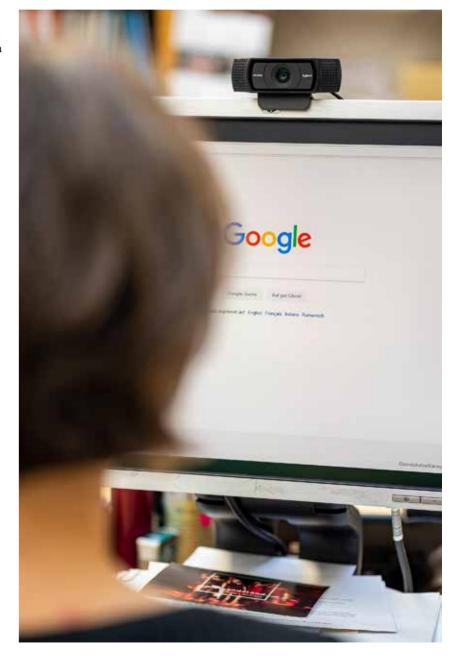
The bill is currently at the parliamentary "resolution of differences" stage, though the transparency provisions are not affected.

Office consultation on the approval of tariff structures in health insurance

The Federal Office of Public Health tried to introduce an exception to the right of access to documents pertaining to the two office consultation procedures on tariff approvals. The Commissioner successfully opposed this.

The Federal Council regularly approves tariff structures for in-patient hospital treatment. In the reporting year, the Federal Council received two such approval requests from the Federal Office of Public Health (FOPH), both of which related to psychiatric care. In these requests, the FOPH proposed that all calculation bases for the tariff structures concerned - as put forward for office consultation – should be excluded from the right of access under the Freedom of Information Act, once approved by the Federal Council. The aim was to protect the business secrets of the parties involved. The Federal Office based its arguments on a provision of the Freedom of Information Act, which states that, by way of exception, "official documents from the office consultation procedure" are still not accessible even after the Federal Council has reached a decision.

During the consultations, we repeatedly called for this proposed rule to be dropped, as the documents in question were prepared or submitted to the FOPH before the start of the office consultation procedure and, for that reason alone, are not "official documents of the office consultation procedure". Consequently, the prerequisites for definitive exclusion from the Freedom of Information Act were not met. Moreover, the Freedom of Information Act already contains specific provision for the protection of business secrets of companies. The FOPH has subsequently waived the special exception.



3.1 Duties and Resources

Services and resources in the field of data protection

Number of staff

Since 2005, the total number of staff responsible for implementing the Data Protection Act has fluctuated between 20 and 24. The reason for the variation is the Freedom of Information Act. which came into force in 2006. Since the Federal Council did not approve additional staff positions as planned, the FDPIC was required to use its 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 legislation in the health sector were passed, they could not all be filled because of general requirements to make savings.

In its dispatch ("report") on the complete revision of the Data Protection Act, the Federal Council promised the FDPIC additional resources in the form of ten staff positions (BBl 2017 7172). Since it is difficult to predict when the parliamentary deliberations on the complete revision will be concluded (see Chapter I), it is currently unclear if and when it will be possible to fill any additional staff positions. Since the new Federal Act on the implementation of Schengen Directive (EU) 2016/680 already covers an aspect of the complete revision and has been in force since 1 March 2019, we have been given additional duties and powers concerning the processing of police-related personal data, which is particularly sensitive (see Chapter 1.2).

Table 4: Staff positions which can be used for Data Protection Act issues

used for	Data Protection Act issues	
2005	22	
2010	23	
2018	24	
2019	24	

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 for the Federal Administration: consultancy, supervision, information and legislation. In the reporting year running from 1 April 2018 to 31 March 2019, the staff resources available for data protection were allocated to these four categories as follows:

Table 5: Services in data protection

Consultancy - private	21,1%	
Consultancy - federal government	21,3%	
Cooperation with cantons	2,1%	
Cooperation with authorities abroad	9,8%	
Total consultancy		54,3%
Supervision	14,1%	
Certification	0,2%	
Data Collection Register	0,7%	
Total supervision		15,0%
Information	17,6%	
Training/talks	5,0%	
Total information		22,6%
Legislation	8,1%	
Total legislation		8,1%
Total data protection		100,0%

One of the consequences of the latest evaluation by the EU is that Switzerland is required to ensure that the federal data protection authorities carry out more frequent checks on the processing of personal data in databases with relevance to Schengen, and to enable this, should be given sufficient resources (see Chapter 1.2).

Consultancy

As set out in the chapter on 'Current challenges', the FDPIC faces a growing demand to provide consultancy services, since he is required to support increasingly large and complex projects. In the reporting period, the increase in the proportion of staff working on consultancy continued to grow, reaching 53.9%. In the FDPIC's 2019 management plan, eleven large projects are currently receiving support in the form of consultancy.

Table 6: Consultancy to large projects in 2018

P 9	
Transport	2
Finance	1
Health and Employment	3
Security	2
Telecommunications/ Internet of Things (IOT)	

FDPIC's resources have not be increased in line with the increased technological risks of re-identification and improper appropriation of data or with the wider challenges digitalisation poses. Therefore, he cannot provide support timewise and 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 have replied to around eighty queries and complaints from members of the public each month with a standard letter. Moreover, the FDPIC 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. As repeatedly stated, we have a limited number of staff, and this severely limits the frequency of the inspections. In 2018, around 12% of staff resources were used for supervisory duties, which is significantly below the long-term average of 20%. In this reporting period, we managed to bring this proportion back up to around 15%, meeting the level of 2016/17. Our 2019 inspection plan shows that another twelve comprehensive inspections can be carried out with these resources. In comparison with the number of large and medium-sized companies in Switzerland (12000), the current frequency of inspections continues to be 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.

The FDPIC
The FDPIC

Legislation

In the Federal Council's dispatch ("report") on the complete revision of the Data Protection Act (BBI 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 had to express its 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 have managed to halt this reduction in this reporting period, 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 Data Protection Act

As outlined above, modern 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. In order to bring legal certainty in relation to the use of these tools and the FDPIC's supervisory role which results, it is essential for them to be anchored in both the GDPR and Swiss data protection law, as the Federal Council proposed in its draft for the completely revised Data Protection Act. Since it is currently difficult to say when the FDPIC will be given the additional staff r promised, our authority must use the new tools as efficiently as possible with the existing staff resources.

Vists to FDPIC offices and hearings by the Control Committees

When the FDJP/FCh subcommittee of the Council of States Control Committee visited the FDPIC's offices in 2018, we presented the results of the pilot project 'Acceleration of Dispute Resolution Process'. In an interview with the subcommittee on 11 April 2019, we had the opportunity to tell them more about the successful conversion of the pilot project to standard procedure.

Assessment criteria

Whether the FDPIC is allocated additional resources in view of the tasks added in the year under review and the results of the latest Schengen evaluation is a matter for the political authorities to decide. Their discretionary judgements play a significant role in assessing current and future digitalisation trends and the impact of these trends on the FDPIC's activities.

The FDPIC's central role is to protect people's privacy and to ensure that they retain ultimate control of their information in the digital society. The FDPIC has 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 objectives against which resources should be measured, broken down by outcome group:

Services and resources in the field of freedom of information

The FoIA 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 has proven to work well in that the proportion of disputes settled amicably remains high and statutory time limits were only exceeded in cases where the procedures and content were complicated. When the number of dispute settlement requests increases, several requests are submitted within a short time period and vacant positions go unfilled, the unit quickly falls behind.

Table 7: Assessment criteria

14515 7. 166666ment of 166114				
Outcome group	Outcome objectives			
Consultancy	The consultancy the FDPIC provides for individuals and for businesses and federal authorities running projects involving sensitive data meets general expectations. 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

Lots of awareness-raising and extensive media coverage

The FDPIC is seeking to increase awareness of the issues of data protection and freedom of information. We will continue seeking more opportunities to engage in dialogue with the public. The website, which attracts around 2000 visitors daily, remains central to communication.

Greater public interest in the FDPIC's work continued in the year under review. Numerous comments by the Federal Data Protection and Information Commissioner and his deputies were reported in the media. Some 3000 opinion pieces and articles were published in the media monitored by the FDPIC, mostly on the subject of data protection as well as transparency in administration. We handled more than 400 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 3500 contacts via these channels. This figure must be viewed with caution, as we switched to a different business management system during the reporting year.

In addition to his media appearances, the Commissioner attended around forty events as a speaker or panellist. The organisers of these events included associations, educational establishments, public authorities, and companies and organisations involved in digitalisation. We also took part in the chat during the Swiss Radio and TV "Dataland" themed evening on 21 November 2018. Furthermore, the FDPIC participated in the second Swiss Digital Day, in the run-up to which he published a video calling on businesses to invest in privacyenhancing technologies when undertaking digital projects.

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 behavioral shift with regard to the use of new technologies.

The FDPIC and the cantonal data protection authorities held a joint media conference in Bern to share information about the privacy-related aspects of elections and the data protection risks inherent in the systematic use of the OASI number. We also engaged in public awareness-raising in the run-up to the entry into force of the Schengen Data Protection Act on 1 March 2019. The focus of this activity was the increased monitoring of the police by the data protection authorities.

Various guidance documents and recommendations published

The Commissioner made a range of more comprehensive publications available in the year under review.

- In May, we issued a guidance document on the EU General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. The first GDPR guidelines issued by the EU authorities were also published at the end of 2018 and shared on Twitter by the FDPIC.
- Raising awareness of data protection begins in the classroom. With the support of the Federal Social Insurance Office (FSIO), in August 2018 we completely updated our teaching materials on this subject. These are aimed at teachers working with pupils aged between 13 and 19.
- In December 2018, in partnership with the cantonal data protection authorities ("Privatim"), the FDPIC published a guide to elections and voting in German, French, Italian and English.
- In January 2019 we issued an overview of the Schengen Data Protection Act.
- On the FDPIC's website we published 18 recommendations on the principle of freedom of information and two on data protection. In addition, we updated a number of fact-sheets and guides, including those on dash cams and transmitting data abroad.

The interactive "Think Data" platform, which is linked on our website, enabled us to raise broader public awareness of 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) in which the FDPIC participated and which he continues to support.

For the first time, the annual activity report is also being published in its entirety in Italian and English. We have also made the report more reader-friendly in terms of layout and text. In a move towards digital publishing, for the first time the report has been created using an ePaper solution.

Website still primary channel for our communication

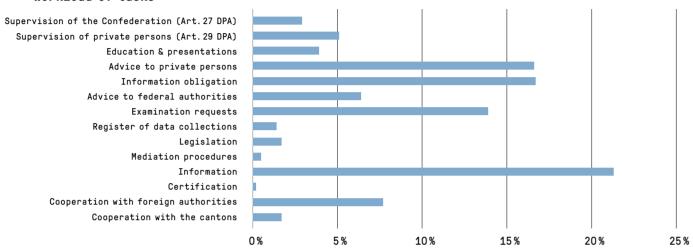
The website is the FDPIC's central communication channel. We attract around 480 000 visitors each year, or 2000 on a single working day. Two out of five visitors are from abroad, mostly from the European countries but also from overseas or Asia. Content is usually available in three languages, German, French and Italian, with some specific content in English. We are planning to gradually optimise our website, making it simpler and more visually appealing and offering users more dialogue formats.

We also communicate via the microblog Twitter at @derBeauftragte. The aim is to make it easier for our followers to quickly access relevant information and be a part of the community that is interested in data protection. We have made the conscious decision not to use other social media platforms.

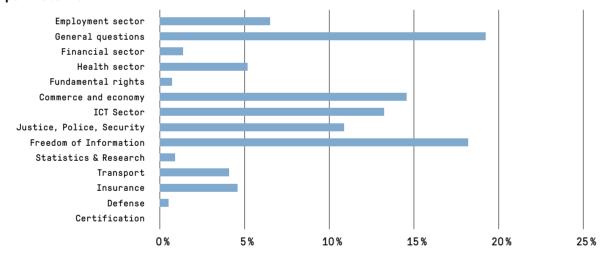
3.3 Statistics

Statistics on FDPIC's activities from 1 April 2018 to 31 March 2019 (Data protection)

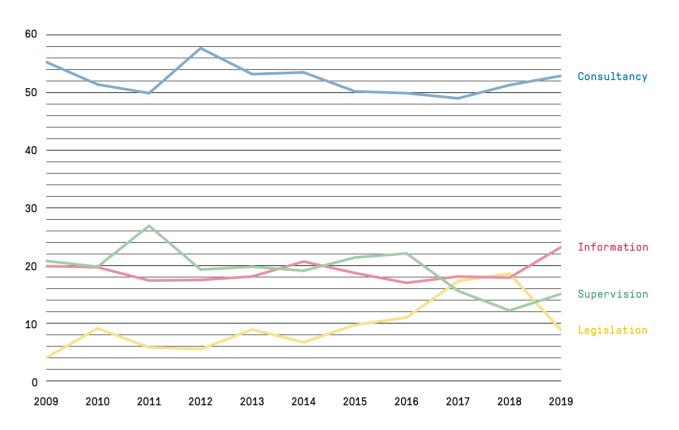
Workload of tasks



Workload per material



Multi-year comparison (as a percentage)



Statistics on applications for access under the Freedom of Information Act from 1 January to 31 December 2018

of Information Act from 1 January to 31 December 2018 Section Reduced Received Rece								
				δ.		anteo		
				rante	F19.	174 OL.		x ⁶ , و
		,	\J.	, ^w b _j	, xî	200	or 60	The L' o'
	ion	^{ر م} م ^ر م	5 4 ¹⁾	es eq	5 Pa'	enc icati	rawn ingre	Cuner
	section	humber of the st	s Roces full	dranted Local Comp.	bccol en	aled Application	Pending res	Wo document are
Federal Chancellery	FCh	18	9	4	4	0	0	1
FCh	FDPIC	7	4	0	1	0	1	1
	Total	25	13	4	5	0	1	2
Federal Department	FDFA	156	107	2	28	6	8	5
of Foreign Affairs FDFA	Total	156	107	2	28	6	8	5
Federal Department	GS FDHA	0	0	0	0	0	0	0
of Home Affairs FDHA	FOGE	2	0	1	1	0	0	0
	FOC	7	2	1	3	1	0	0
	SFA	6	6	0	0	0	0	0
	METEO CH	0	0	0	0	0	0	0
	NL	0	0	0	0	0	0	0
	FOPH	42	15	4	11	2	10	0
	FS0	5	1	3	1	0	0	0
	FSI0	11	7	0	1	1	1	1
	FSV0	15	8	1	4	0	1	1
	SNM	0	0	0	0	0	0	0
	SWISS MEDIC	24	9	2	3	2	8	0
	SUVA	0	0	0	0	0	0	0
	Total	112	48	12	24	6	20	2
Federal Department	GS FDF	23	12	7	2	0	0	2
of Finance FDF	FITSU	3	1	0	2	0	0	0
	FFA	0	0	0	0	0	0	0
	FOPER	1	1	0	0	0	0	0
	FTA	7	3	2	0	0	1	1
	FCA	6	3	1	0	1	1	0
	FOBL	6	5	0	0	0	1	0
	FOITT	0	0	0	0	0	0	0
	SFA0	19	5	7	3	0	0	4
	SIF	0	0	0	0	0	0	0
	PUBLICA	0	0	0	0	0	0	0
	CCO	3	2	0	1	0	0	0
	Total	68	32	17	8	1	3	7

				×e ⁸				
				aranted	*ely	574 dray.		ex. ^S
	section	Wilder of Feduce	, s Access tull	A Granted Long	bcc or	ishily drafted heptication	to bedjug teg	ho doomert
Federal Department	GS FDJP	5	3	0	0	0	0	2
of Justice and Police	FOJ	3	3	0	0	0	0	0
FDJP	FEDPOL	4	3	1	0	0	0	0
	METAS	2	2	0	0	0	0	0
	SEM	13	7	1	2	0	1	2
	PTSS	1	1	0	0	0	0	0
	SICL	1	1	0	0	0	0	0
	IPI	0	0	0	0	0	0	0
	FGB	1	1	0	0	0	0	0
	ESchK	2	1	1	0	0	0	0
	FAOA	0	0	0	0	0	0	0
	ISC	1	1	0	0	0	0	0
	NCPT	0	0	0	0	0	0	0
	Total	33	23	3	2	0	1	4
Federal Department of the Environment,	GS DETEC	5	4	1	0	0	0	0
Transport, Energy	FOT	27	10	0	15	2	0	0
and Communications DETEC	FOCA	6	2	0	3	0	0	1
-2120	SF0E	12	11	1	0	0	0	0
	FEDRO	6	5	0	0	0	1	0
	OFCOM	10	4	0	3	0	0	3
	FOEN	10	3	0	1	0	3	3
	ARE	3	1	1	0	0	0	1
	ComCom	1	0	0	1	0	0	0
	ENSI	20	10	1	2	6	1	0
	PostCom	3	3	0	0	0	0	0
	ICA	2	2	0	0	0	0	0
	Total	105	55	4	25	8	5	8

Statistics on applications for access under the Freedom of Information Act from 1 January to 31 December 2018

				nted and	24	granted	~drawr	
		. K	ران.	des coub	ost.	ralia riv	or with	lest's sent
	section	hunde of other	, koces full	oce socied	Vcc or	ally hanked hopicati	on ithirdrawn Pendind ref	No gocru
Federal Department	GS DDPS	6	5	0	1	0	0	0
of Defence, Civil Protection and Sport	Defence / Army	14	6	0	4	1	3	0
DDPS	FIS	9	2	2	2	1	2	0
	armasuisse	6	4	0	0	0	2	0
	FOSPO	4	3	0	0	0	1	0
	FOCP	2	2	0	0	0	0	0
	swisstopo	0	0	0	0	0	0	0
	OA	0	0	0	0	0	0	0
	Total	41	22	2	7	2	8	0
Federal Department of Economic Affairs,	GS EAER	6	3	2	1	0	0	0
Education and	SECO	12	4	3	4	0	0	1
Research EAER	SERI	11	8	3	0	0	0	0
-ALN	FOAG	17	4	3	6	1	1	2
	FONES	2	1	0	1	0	0	0
	FH0	0	0	0	0	0	0	0
	PUE	6	5	0	1	0	0	0
	COMCO	20	12	4	4	0	0	0
	ZIVI	2	2	0	0	0	0	0
	FCAB	1	1	0	0	0	0	0
	SNSF	1	0	1	0	0	0	0
	SFIVET	2	2	0	0	0	0	0
	ETH Board	16	10	2	3	0	1	0
	Innosuisse	0	0	0	0	0	0	0
	Total	96	52	18	20	1	2	3
Office of the	OAG	8	3	2	0	0	2	1
Attorney General OAG	Total	8	3	2	0	0	2	1
Parliamentary Services	PS	3	0	2	0	0	0	1
PS	Total	3	0	2	0	0	0	1

Overview of applications for access per Department and the Federal Chancellery

Department.	winder of	, x ⁵	kcess to	14 drantad	Pcc Serie	nletel ⁴	bcc of	cially graded	kopi jestio	Sar	Pending ref	lues ^{ts}	Wo document	L availab
FCh	25		13		4		5		0		1		2	
FDFA	156		107		2		28		6		8		5	
FDHA	112		48		12		24		6		20		2	
FDF	68		32		17		8		1		3		7	
FDJP	33		23		3		2		0		1		4	
DETEC	105		55		4		25		8		5		8	
DDPS	41		22		2		7		2		8		0	
EAER	96		52		18		20		1		2		3	
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)	-	
Total 2009 (%)	232	(100)	124	(53)	68	(29)	40	(17)	0	(0)	-		-	

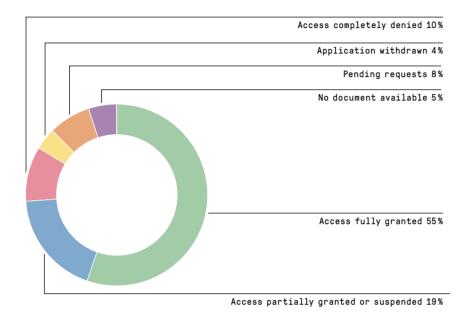
Number of requests for mediation

Category of applicant	2018
Media	24
Private persons (or no exact assignment possible)	26
Interested parties (associations, organisations, companies, etc.)	9
Lawyers	4
Companies	13
Total	76

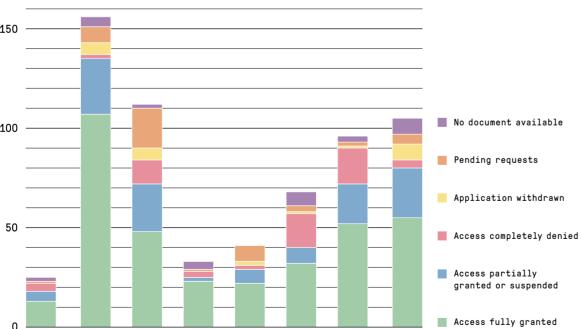
85

The FDPIC Organigramm

Overview applications for access in the federal administration







EAER

DETEC

FCh

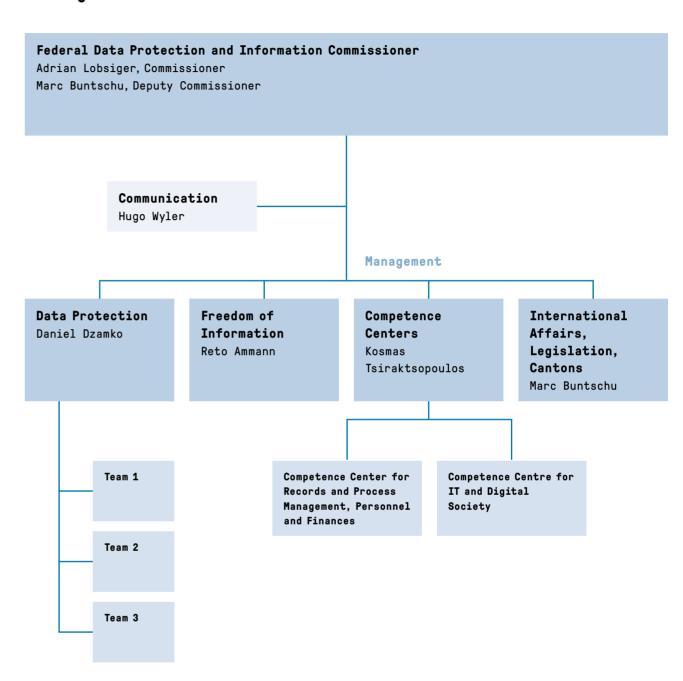
EDA

FDFA

FDJP

DDPS

3.4 Organisation (Status 31 March 2019)



Abbreviations

Abbreviations

ADR Alternative Dispute Resolution body
AEOI Automatic exchange of information
AFAPDP Association of French speaking data protection authorities
CNIL French data protection Authority
DETEC Federal Department of the Environment, Transport, Energy and Communications
DoC Department of Commerce
EAER Federal Office of Economic Affairs, Education and Research
EDPB European Data Protection Board
EDPS European Data Protection Supervisor
E-ID Act Federal Act on Recognised Electronic Means of Identification

Eurodac EU fingerprint database for identifying asylum seekers

ute Resolution body FADP Federal Act on Data Protection

FCh Federal Chancellery

FDFA Federal Department of Foreign Affairs

FDJP Federal Department of Justice and Police

FIS Federal Intelligence Service

FolA Freedom of Information Act

FPISA Federal Act on the Police Information Systems

GDPR General Data Protection Regulation of the EU

IRM Independent Recourse Mechanism

ISA Federal Act on the Intelligence Service

OASI Old-age and survivors' insurance

OECD Organisation for Economic Co-operation and Development

OFCOM Federal Office of Communications

PCLOB Privacy and Civil Liberties
Oversight Board

PCTA Federal Act on Police Counterterrorism Measures

PIC Political Institutions Committee

Privatim Conference of the cantonal data protection commissioners

RIPOL Computerised police search system

SDPA Schengen Data Protection Act

SIS Schengen Information System

TAAA Federal Act on International Administrative Assistance in Tax Matters

VIS Visa Information System

Figures

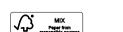
Images
ps architektur, perroneschneider GmbH,
4051 BaselCove
Terres des Hommes Schweiz,
4018 Baselp. 19, 66, 7
Die Medienmacher AG,
4132 Muttenz p. 25, 34, 38, 52, 5
restudio AG,
4053 Baselp. 31, 59
Duplex Design GmbH,
4053 Basel p. 4

88

Impressum

This report is available in four languages and also in an electronic version on the Internet. Distribution: BBL, Verkauf Bundespublikationen, CH-3003 Bern www.bundespublikationen.admin.ch Art.-Nr. 410.026.e

Layout: Duplex Design GmbH, Basel Photography: Maya Valentin Characters: Pressura, Documenta Print: Ast & Fischer AG, Wabern Paper: PlanoArt®, woodfree bright white



Key figures

Workload data protection

Legislation

Information

15 % Supervision

54.3%

pending

Applications for access (FoIA) Freedom of Information

granted

partially granted

or suspended

withdrawn

0ther

5 %

No document available

Medial resonance

0ther

2 %

Contributions Dedication/ examined Engagement* Type of media Tonality Countries Languages Online news German 74% Positive 9 % Switzerland 76% French 13% Newspapers 12% Negative 10 % Germany Twitter 19% Italian 8% Neutral 81% USA 3 % Blogs 10% English 5 % Hungary 2 % ■ TV/Radio 1% 8 % Other 1% France

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.



No data collection on stock, but



Proportionality



only as far as necessary to achieve the purpose. Data processing is limited in scope and time.



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



Responsibility

4

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



^{*}Number of all examined contribution interactions (Likes, Retweets, etc.)