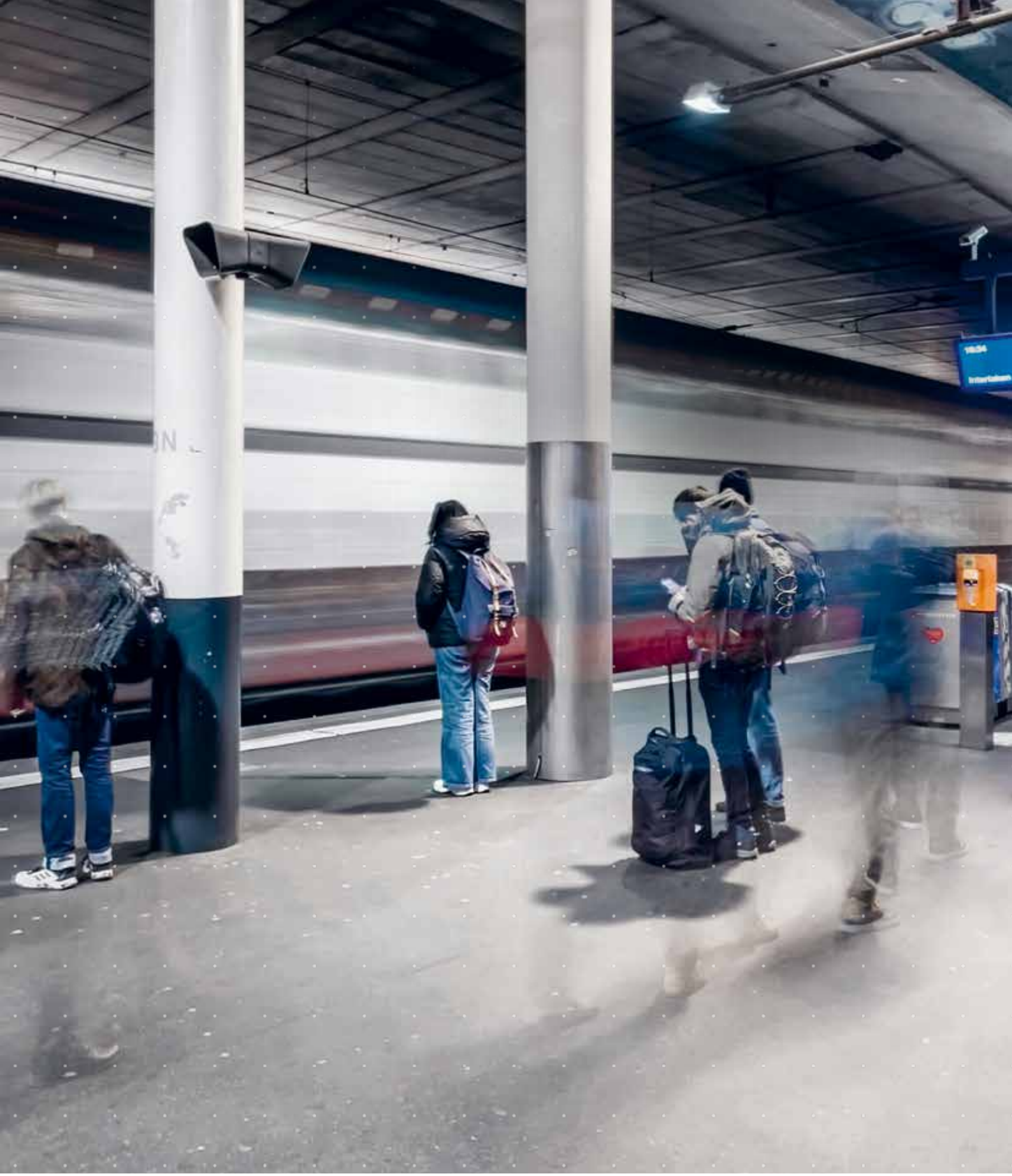


29th Annual Report 2021/22

Federal Data Protection and Information Commissioner

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Annual Report 2021/2022

Federal Data Protection and Information Commissioner

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

This report covers the period between 1 April 2021 and 31 March 2022.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Foreword

As we approach what we hope is the end of a pandemic that has severely impacted public health and personal freedom, the Digital Switzerland strategy can be said to have made great strides in data protection with the Covid app and the Covid certificate along with its light version. Thanks to their decentralised and data-minimised design, these tools have helped prevent individuals' personal data from having to be transmitted to the Federal Administration. Furthermore, the disclosure of health data to private individuals has been limited to an acceptable level in compliance with data protection requirements.

At the same time, Digital Switzerland is coming to terms with technical and organisational failures in the operation of certain contact tracing apps and vaccination, organ donor and breast implant registers. After investigative journalists exposed just how easy it was to gain unauthorised access to sensitive personal data, all platform operators will by now be well aware – if they were not already – of how crucial it is that they take the necessary action to live up to their responsibilities. Equally significant is the fact that, after a failed attempt, the overdue implementation of a state-recognised electronic identity is now going ahead.

The digitalisation of our working and private lives has been accelerated by the pandemic. Furthermore, the recent announcement of a 'Metaverse' rollout marks the beginning of work to replace today's app-based social media platforms. Next-generation internet-based networking will see people meeting in virtual worlds using ultra-light VR headsets. Their physical environment will be overlaid with digital content and thus transformed into 'augmented reality'. How will these VR headsets capture our private surroundings? How will cloud-based artificial intelligence capture and interpret our gestures and facial expressions, our voices and our overall demeanour? Will it just be a matter of time before people perceive the non-digital, natural world as grey, lonely and threatening?

These questions posed by the Confederation's supervisory authority for data protection matters reflect the people's entitlement to help shape their digital future.

Adrian Lobsiger
Federal Data Protection and Information Commissioner

Bern, 31 March 2022

Freedom of Information

The FDPIC

Current Challenges

I Digitalisation

The vast majority of people in Switzerland use information and communication technologies (ICT) every day. Digitalisation has permeated all areas of society. However, this phenomenon is not expected to reach a saturation point but instead to continue as a process of progressive evolution of digital reality.

Are smartphones about to reach their peak?

This process of progressive evolution is best exemplified by the smartphone, which has played a key role in the digitalisation of society over the past 15 years. The amount of data generated via this device increased further during the year under review, mainly because people seeking access to restaurants and public events were required to present a COVID-19 certificate for several months and therefore acquired the habit of always carrying their smartphones switched on when moving in public spaces. That said, the vision of a 'metaverse' frequently dominating media headlines suggests that smartphones are about to reach their peak as well: Promoters of this vision claim that people will gradually move away from today's app-based social media platforms – including screen, mouse and keyboard – to meet up in virtual spaces wearing a simple headset.

The 'metaverse' versus the real world

During the year under review, in order to attract users and investors with a view to claiming its stake in the future global metaverse and establishing commercial rights, the global communications group Facebook changed its name to 'Meta'.

Next-generation internet networking will see people wearing ultra-light VR headsets and meeting in virtual spaces, in which their physical environment is overlaid with digital content and thus transformed into a mixed, enhanced world referred to as 'augmented reality'. The idea is that people will perceive this new environment as real from a sensory point of view even though the digital avatars through which they meet in the 'metaverse' are not flesh and blood. People will be able to meet this way both in their private homes and at work. To make this possible, sensors will scan and measure the private walls and send the data obtained via the internet in real time. This alone illustrates the extent to which the 'metaverse' aims to invade the privacy of billions of people.

Anyone will be able to immerse themselves in the metaverse within seconds simply by donning a pair of inconspicuous glasses. The effect that this will have on the amount of time spent in the natural world, without digital animation, can be inferred from the behaviour of users of virtual reality games. When people end up perceiving the real world, without digital animation, as grey and lonely, they will inevitably spend far less time there. Will meta-society ever go as far as considering a stroll through the world without digital animation as threatening because of a lack of certain warning signs?

To implement 'augmented reality', the sensors fitted in the glasses will track eye movement, voice, gestures, facial expressions and posture, right down to reading and food intake of those wearing the glasses. All this sensitive data will eventually end up in the cloud of the social network operators, of course on an even more gigantic scale than is the case in today's digital world.

However, the more people transfer their social lives to digitally animated environments, the greater the risk of their privacy being violated. This is the case, for example, with the use of photorealistic avatars, which

"The concept 'Metaverse' aims to invade the privacy of billions of people."

will be perfected in just a matter of time. In this context, the FDPIC and other supervisory authorities will be involved at an early stage to ensure that providers of digitally animated environments clearly state the associated risks and take action to protect individuals' rights to privacy and self-determination.

Digital Switzerland Strategy

In order to ensure that people in Switzerland can benefit from digitalisation, the Federal Council meets regularly to formulate a Digital Switzerland Strategy. This strategy encourages the authorities at all federal levels as well as members of civil society, businesses, the scientific community and government to work together to promote the digital transformation.

According to the Digital Switzerland Strategy, the digital transformation of existing structures requires a rethinking of traditional ways of living and doing business together. This calls for digital skills and networking and data sharing between all stakeholders. This pooling of knowledge is expected to create a Switzerland in which people are prepared to participate digitally in social, economic and political life.

Public service as a discrete partner of the population

Many promoters of the digital transformation counterpose this strategic vision to the frowned-upon practice of storing data in so-called 'silos', associated with outdated thinking and stereotypical backward-oriented administration in Bern. Unfortunately, it is all too easy to overlook the fact that information barriers considered obsolete can indeed be inbuilt pillars of the modern state governed by the rule of law. The state governed by the rule of law replaced the aristocracy, in which all responsibilities of public administration were determined by the power of a prince. The prince could take charge of any business at any time, obtain any information whatsoever, and take care of matters concerning his subjects personally and autonomously. It was only with the introduction of a separate, independent judiciary, in accordance with the principle of the rule of law, and the division of the administration into various different specialist offices with exclusive knowledge, that the conditions were created for the state to become a 'public service' and for subjects to become citizens.

Today's state with its separation of powers is a conglomeration of service facilities supporting members of the public in exercising their civil rights and duties under special laws. The specialisation of administration and the segmentation of official information have gone hand in hand with a transformation of the state's power over civil society: today, civil society confidently asserts its rights and expects professional, discrete services from the various specialist offices in return for taxes paid, and, if necessary, it is prepared to defend its rights in a court of law.

The state governed by the rule of law focuses on developing a network of factual data rather than citizens' data

In this historical context, data protection must support the strategic need for increasing involvement of the state and administration in the dissemination, sharing and use of data in the digital network in various different ways. Data protection must ensure that this surge of information does not focus on personal data but on factual data and that information restrictions are observed in accordance with the rule of law. These restrictions enable civil society to assert its civil rights vis-à-vis the authorities.

"When people end up perceiving the real world as grey and lonely, they will inevitably spend far more time in 'Metaverse'."

Data protection is about protecting the individual's fundamental rights, which are denied to citizens of authoritarian states. To this day, the administration in such states restricts citizens' access to offices, subsidies, education, social benefits and medical care by providing an incomprehensible amount of official information and data sources. Digital networks and low-cost surveillance technology have enabled authoritarian states to intensify their control over citizens to an extent that will hopefully frighten the West for a long time to come. In its draft legislation on artificial intelligence, the European Commission felt it necessary to prohibit EU Member States from permanently monitoring citizens in the sense of 'social scoring' or employing large-scale real-time facial recognition systems in public spaces.

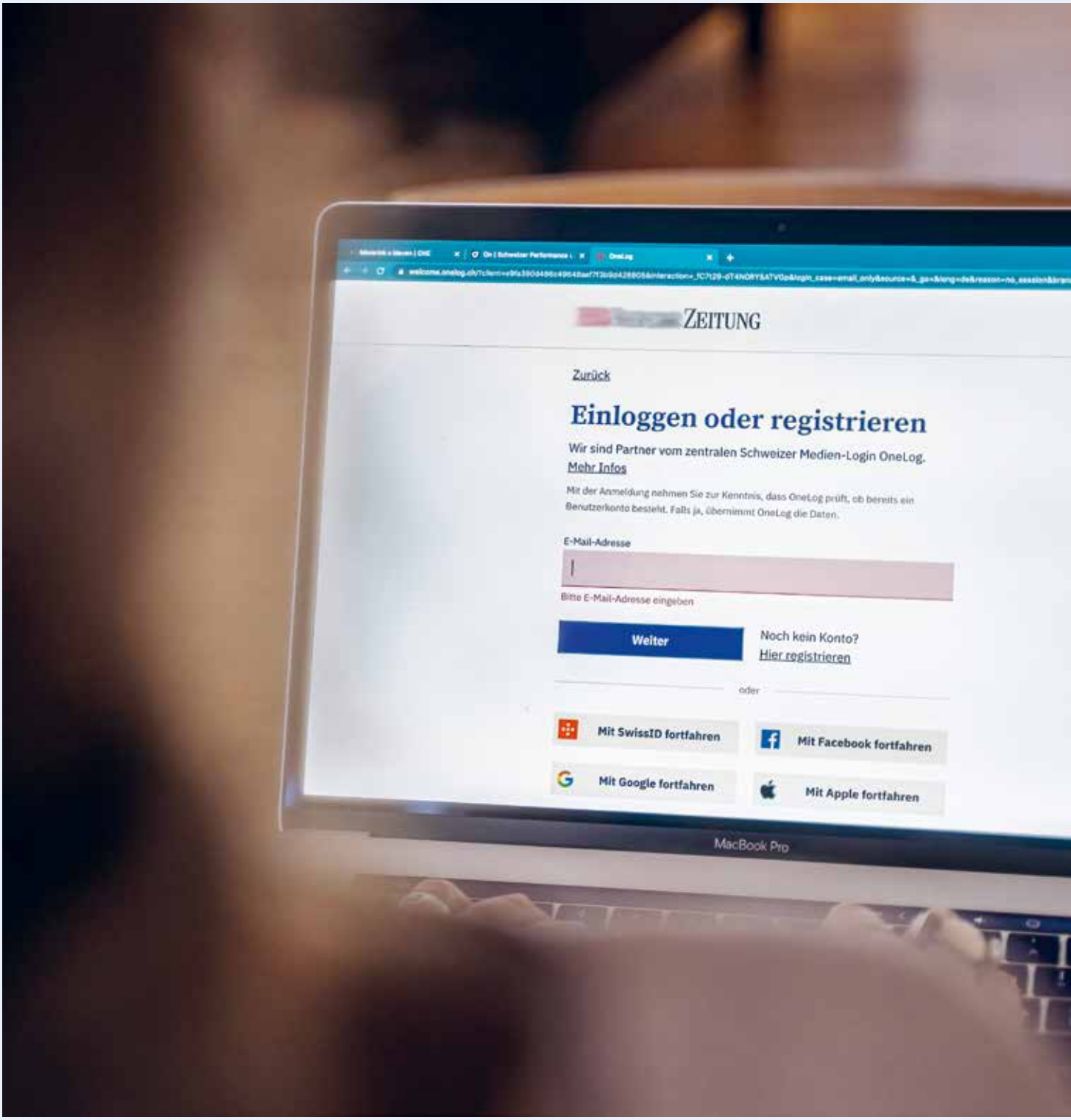
Anonymous communication is a civil right, never an 'abuse of freedom'

From a data protection perspective, it is equally important that Western democracies preserve the right of private individuals to process their own data and that of their customers autonomously and, at their own discretion, to prevent third parties – including the state – from accessing it. Crime is an intrinsic part of society and can therefore never be used to justify the untenable accusation that citizens are 'abusing their freedom' when they communicate via secure systems. If a person first goes to a restaurant on foot and then takes a bus to the place where they subsequently commit an intentional crime, they cannot be accused of abusive movement in public spaces, abusive food intake or abuse of public transport. The same applies if a criminal exchanges information via secure channels before or after committing a crime. In the free world, everyone should be entitled to move around anonymously in the analogue and digital worlds without being incriminated by their own statements. Technology companies that use artificial intelligence to monitor the mobile phones that they sell for illegal content in order to report the owners to the police have no place in the free world.

However, the right to communicate anonymously does not prevent the police from being able to take action in specific cases against individuals, or their associates, who are suspected of committing a crime if they have sufficient evidence and a court warrant.

However, if private companies or individuals in Switzerland are prevented from protecting their private information or that of their customers against third parties without a sufficiently clear legal basis, the FDPIC will oppose this within the scope of his legal powers. In this respect, the FDPIC calls for digital strategies to be implemented with caution and in a differentiated manner in such a way that they enhance the private lives of people in Switzerland and strengthen self-determination rather than undermine them.

"Data protection is about protecting the individual's fundamental rights, which are denied to citizens of authoritarian states."


ZEITUNG
Zurück
Einloggen oder registrieren
Wir sind Partner vom zentralen Schweizer Medien-Login OneLog.
Mehr Infos
Mit der Anmeldung nehmen Sie zur Kenntnis, dass OneLog prüft, ob bereits ein Benutzerkonto besteht. Falls ja, übernimmt OneLog die Daten.
E-Mail-Adresse
Bitte E-Mail-Adresse eingeben
Weiter
Noch kein Konto?
Hier registrieren
oder
Mit SwissID fortfahren
Mit Facebook fortfahren
Mit Google fortfahren
Mit Apple fortfahren
MacBook Pro

II Consultancy, supervision and mediation

In his role as a supervisory body, the FDPIC 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's data protection officers and to the state data protection authorities. Following this approach, in our supervisory capacity, we have continued to support many big data projects run by federal authorities and private companies and have promoted the responsible use of modern working tools such as the data protection impact assessment as well as the employment of data protection officers in companies.

Supervision can only partly meet the public's legitimate expectations

After declining significantly in the 2015/16 period, expenditure on supervisory duties has been increased again slightly by the FDPIC in recent years, although it has stabilised at a low level due to ongoing under-resourcing. During the year under review, our authority was again unable to meet the public's legitimate expectations to the extent that it would have liked (see Section 3.1). Although the FDPIC further strengthened cooperation with the National Cyber Security Centre during the reporting year, he still lacks sufficient resources to perform the systematic random checks and technical security inspections that would be particularly useful for the storage of sensitive health data. In this context, it is worth remembering the case of the Myvaccines foundation (currently in liquidation) and, during the year under review, the cases of uncontrolled access to the organ donor and breast-implant registers (see Section 1.4).

Increase in mediation requests causes a processing backlog

As an information commissioner, the FDPIC had to temporarily suspend his oral mediation activities during the reporting period due to the pandemic, which resulted in fewer amicable outcomes. Consequently, the FDPIC found himself having to provide more written recommendations, which, combined with an increase in the number of mediation requests, meant that statutory processing deadlines could not be met in many procedures with the staff resources available. With mediation requests set to increase and without additional resources, this negative trend is likely to be become more pronounced, making swift processing, as required by law, increasingly difficult to achieve.

"Digital strategies has to be implemented with caution and in a differentiated manner in such a way that they enhance the private lives of people and strengthen self-determination rather than undermine them."

III National and international cooperation

National cooperation

As digitalisation forges ahead, cloud computing is among the items on the agenda of the FDPIC and the cantonal data protection authorities. For example, privatim – the Conference of Swiss Data Protection Commissioners – has completely revised its fact sheet on cloud-related risks and measures and adopted the new version in February 2022. The FDPIC had previously commented on the draft in an advisory capacity. Here too, cooperation was good because of the good working relationship. The FDPIC focused, in particular, on the topic of cloud computing within the Federal Administration (see Section 1.1).

Council of Europe

The FDPIC continues to be actively involved in the Council of Europe, attending all the meetings of the Convention 108 Consultative Committee responsible for data protection. In 2021, the Committee of Ministers of the Council of Europe adopted two documents which the Consultative Committee had worked on: the Declaration on the need to protect children's privacy in the digital environment, and the update of the Committee of Ministers' recommendation on profiling.

International cooperation

The disclosure of personal data to a country with an inadequate level of data protection is an issue that raises similar questions in a number of countries. The FDPIC is monitoring developments in this area in EU and EEA Member States. For example, among other things, he has examined the modified standard contractual clauses published by the European Commission to determine the extent to which he can recognise these in Switzerland (see Section 1.8).

Evaluation of the level of data protection

There has been a further delay in the publication of the long-awaited report by the European Commission on the adequacy of the level of data protection in Switzerland. In the meantime, the existing adequacy decision of the European Commission under the EU Data Protection Directive 95/46/EC (replaced by the GDPR) remains in force. The EU Commission is expected to publish the adequacy reports on all the states that were already considered adequate pre-GDPR at the same time. It is hoped that the reports will be published before the end of 2022.

Data protection

1.1 Digitalisation and fundamental rights

DIGITAL TRANSFORMATION OF THE ADMINISTRATION

In many of the Federal Administration's digitalisation projects, the FDPIC worked to ensure privacy-compliant implementation

The Federal Administration's many digital transformation projects pose a challenge for the FDPIC as a small authority. In an advisory and supervisory capacity, the FDPIC works to ensure that privacy is systematically implemented from the start. In performing his role, he maintains contact with the new Digital Transformation and ICT Steering (DTI) Service of the Federal Chancellery, the Federal Office of Information Technology (FOITT) and the federal offices responsible for the projects so that he can be informed of their digitalisation projects at an early stage and stay abreast of ongoing and future projects.

The Federal Administration's cloud strategy, which aims to allow the use of cloud services, is a key part of the digital transformation. The FDPIC commented on the motions concerning the sourcing of public cloud services from US and Chinese companies and the use of Microsoft cloud services. He also specified the data protection requirements for the use of cloud services by the public authorities (see Focus II).

After the E-ID Act was rejected in the referendum of 7 March 2021, the FDJP quickly resumed its legislative work for a new e-ID concept. The FDPIC seized the opportunity to provide specialist input and also expressed his main concerns in public (see Section 1.1).

The bill for the Federal Act on the Use of Electronic Means for the Performance of Official Duties (EMBaG) aims to promote the electronic handling of federal business processes based on the 'digital first' approach. During the office consultation, the FDPIC took a critical look at the various regulations. In particular, we were able to effect changes with regard to the pilot procedures, the ensuring of an adequate level of data security, accountability and the Federal Statistical Office's access to data for statistical purposes (see Section 1.1).

The aim is to collect data once only and then reuse it and share it (once-only principle and reuse of data). This project involves risks for citizens as well as opportunities, as seen in the pilot project involving the collection of tax data, on which the FDPIC effectively expressed his concerns (see Section 1.1).

Sector-specific projects

Large-scale sector-specific digitalisation projects associated with high privacy risks include the complete revision of the Customs Act and the partial revision of the Intelligence Service Act (IntelSA). Both projects involve modernising the IT systems in particular. The FDPIC followed the customs project closely, and significant improvements were achieved from a data protection perspective (see Section 1.2). During the consultation process, the FDPIC was also able to achieve many improvements to the IntelSA (see Section 1.2).

The most important digitalisation project in the healthcare sector is undoubtedly the implementation of the electronic patient file, which has suffered major delays. The FDPIC is

following the implementation work and maintains a close dialogue with the authorities and private-sector actors responsible on the data protection challenges. During consultations, he commented on the further development of the legal framework and systems.

The data protection risks associated with the digital transformation are not limited to the general public but also affect employees of the Federal Administration. In reference to a planned pilot project for the creation of a know-how network, the FDPIC commented on the data protection framework and on further action (see Section 1.1).

DIGITAL TRANSFORMATION

Federal act on the use of electronic means for the performance of official duties

The FDF has submitted to the FDPIC for consultation the draft federal act on the use of electronic means for the performance of official duties (EMBaG), which sets out a number of goals in connection with the digital transformation of the Federal Administration. The FDPIC has commented, requesting various improvements and clarification, which the Federal Administration has agreed to implement.

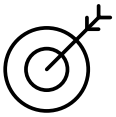
With a cross-sectional act such as the EMBaG, the Federal Administration aims to achieve an effective, modern use of data beyond the confines of the administrative units as part of the digital transformation of the Federal Administration and the expansion of its digital services. The bill regulates various aspects such as the bases for the publication of freely accessible government data (open government data), the provision and use of information and communication technology resources by the federal authorities, the principle of automated electronic data exchange via interfaces and the operation of an interoperability platform.

The FDPIC acknowledges the Federal Administration's digital transformation mandate and recognises the benefits of digital data interoperability. However, he also regularly points out the need to promptly recognise and identify the risks to the rights of the individuals concerned associated with the implementation of these goals. In his opinion on the EMBaG, the FDPIC therefore repeatedly stresses the need to create a data protection impact assessment. The bill and its various requests do not distinguish clearly enough between factual data and personal data, making it often difficult to draw a line between the act in question and the Federal Act on Data Protection. Therefore, the FDPIC has requested clarification on various points.

No extended access to data

In connection with the once-only principle and the reuse of data, as part of the EMBaG bill, a legal basis has been established in the Federal Statistics Act allowing the Federal Statistical

Office (FSO) to access data already held by third-party authorities via the internet unless otherwise provided by a different act. In that regard, the FDPIC demands that access be strictly limited to data that the FSO requires for its statistics, stating that the new procedure must not extend access to personal data. He also demands that the legislative dispatch on the EMBaG explicitly set out an obligation for the federal bodies concerned to exclude from access all data not required by the FSO, particularly personal data. The Federal Council will therefore need to specify in detail in an ordinance which bodies will be required to give the FSO online access to which type of data in which areas.



In order to promote the digital transformation of the Federal Administration, the bill also set out to establish the basis for conducting pilot tests, particularly for technical innovations. In this context, the FDPIC pointed out that pilot tests are to be conducted primarily in accordance with Article 35 of the revised FADP provided that the conditions for application of the act are met. Outside the scope of this act, pilot tests conducted in accordance with the EMBaG may be approved by the competent department after obtaining the opinions of the FDPIC and other offices. The bill also provides that the data subjects are to be informed in advance about the planned data processing as part of the pilot test and allowed to choose whether or not to give their consent, which the Commissioner welcomes.

Following the consultation, the offices responsible took all our comments on board and have already amended the bill accordingly or plan to do so. The FDPIC will continue to monitor the implementation of the various projects.

NATIONAL DATA MANAGEMENT PROGRAMME

The FDPIC criticised the tax data survey

The FSO submitted to the FDPIC a draft amendment to the Ordinance on the Conduct of Federal Statistical Surveys, which provided for a new tax data survey. Given the significant privacy risks involved in the project, the FDPIC demanded that a proper risk assessment be carried out.

One of the first projects to be carried out as part of the national data management (NaDB) programme is the introduction of a tax data survey by the Confederation. The project envisages allowing the use of administrative data held by the Federal Tax Administration (FTA) and tax data held by the cantonal tax administrations for federal statistical purposes in accordance with the once-only principle (see 28th Annual Report, section 1.1).

With a view to implementation, the Federal Statistical Office (FSO) – which is leading the project – submitted to the administrative units a draft amendment to the Annex to the Ordinance on the Conduct of Federal Statistical Surveys in summer 2021. Among other things, it introduced a new tax data survey, which involved collecting all income and wealth tax data on natural persons and all profit and capital tax data on legal entities from the cantons every year. The FTA was appointed as the organ responsible for conducting the survey. The non-anonymised

data would thus be available to both the FTA and the FSO for statistical purposes.

During the office consultation, the FDPIC criticised the project design. He pointed out that tax data provided a comprehensive picture of an individual and, therefore, the project constituted a significant encroachment on their privacy. The project involved processing large amounts of data, including particularly sensitive personal information such as religious beliefs, health data, social assistance etc., on all taxpayers in Switzerland. Analysing the data of each taxable subject for statistical purposes could lead to profiling and is therefore deemed high risk. The fact that the FTA and the FSO could analyse the same data sets for various statistical purposes further increases this risk. On that basis, the FDPIC demanded that the FSO first conduct a proper risk assessment, i. e. that it identify and assess the risks involved and define the measures required to tackle them. Furthermore, the FDPIC pointed out that the principle of purpose limitation had to be observed, especially in projects involving the reuse of data. According to this principle, the FTA, in particular, had to ensure, at all times, the technical and organisational separation of data used for supervisory purposes from data used for statistical purposes. Finally, the FDPIC also expressed concerns as to whether the current legal basis for federal statistics still met the requirements of the principle of legality.

After this office consultation, there was an oral exchange between the FSO and the FDPIC. In September 2021, the FSO subsequently informed the FDPIC that the tax data survey was no longer among the planned changes to the Annex to the Ordinance on the Conduct of Federal Statistical Surveys.

DATING APPS

Analysis of data processing activities

The FDPIC continued his investigation into a Swiss dating app.

In spring 2021, the FDPIC began a case investigation into a Swiss dating app provider after receiving reports of app users experiencing difficulty having their accounts deleted at their request. As well as seeking clarification on this issue, our investigation focused on the disclosure of personal data to third parties and compliance with transparency and data security requirements (see 28th Annual Report 2020/2021, Section 1.1).

During the year under review, the FDPIC established the facts and submitted them to the provider for comments. The matter was subsequently settled with the provider, and the FDPIC is now carrying out a legal analysis of his findings, which was still ongoing at the time of writing this annual report.

Preparations for the entry into force of the revised FADP

In spring 2021, the FDPIC published an overview of the key changes introduced by the revised Federal Act on Data Protection of 25 September 2020 on his website. The FDJP has announced that the Federal Council will be asked to bring the act into force on 1 September 2023 instead of in the second half of 2022 as originally planned.

In summer 2021, the Federal Office of Justice (FOJ) presented the FDPIC with a first draft of the implementing ordinance relating to the new FADP. Since then, the FDPIC has expressed his concerns in various opinions. At the end of the year under review, not all the points identified by the FDPIC as requiring improvement had been resolved.

In parallel with this advisory work on legislative issues, the FDPIC is forging ahead with the creation of three digital portals. These will allow efficient handling of data processing records, data security breaches and the legally required notifications of company data protection officers. The FDPIC's website is also being updated (see Section 3.2).

REVISION OF THE DPO

New ordinance to the revised Federal Act on Data Protection

Work on a new ordinance to the revised Federal Act on Data Protection is in full swing. The FDPIC presented his concerns to the Federal Office of Justice, which is leading the work.

The FDPIC first received a draft ordinance to the revised Federal Act on Data Protection for consultation in summer 2020. Since then, he has expressed his views in a number of opinions and meetings and has exchanged views with the Federal Office of Justice (FOJ, leading the work) on the provisions that he felt needed improving. However, the FDPIC feels that there are still many points that need to be improved. He understands the criticism expressed by participants of the public consultation in many respects and has urged the FOJ to take it into account in the upcoming work on the draft. The PIC-N and PIC-S also demanded changes after the consultation and after consulting the FDPIC. Work on the revision of the ordinance to the Federal Act on Data Protection was still ongoing at the end of the year under review.

Insufficient detail

In the FDPIC's view, the implementing provisions on data protection impact assessments (DPIAs), profiling, automated decision-making and charging systems are still full of loopholes and provide insufficient detail, making it difficult to apply the law in accordance with the principle of legal

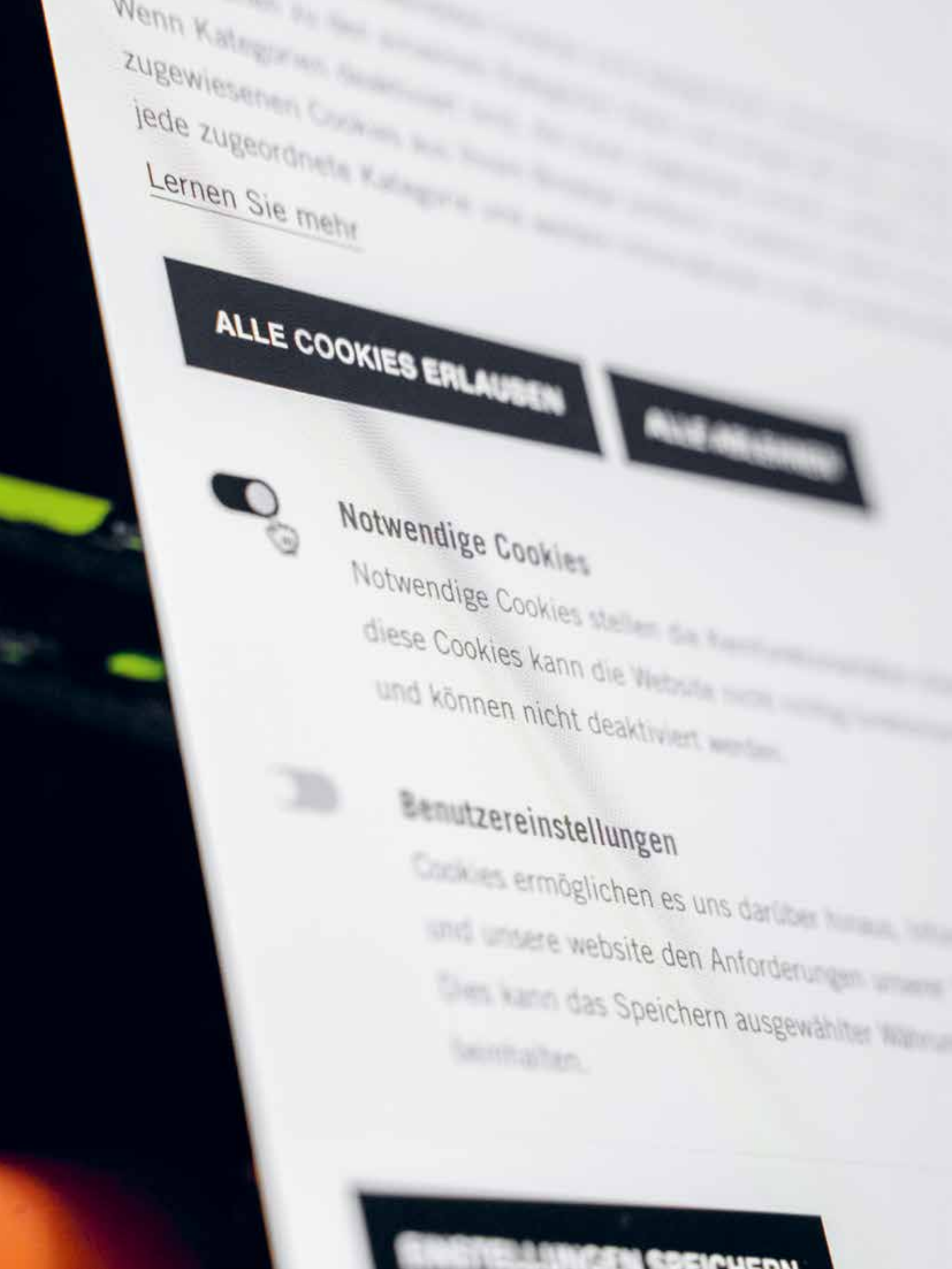
certainty. In particular, the current draft ordinance does not cover the key tool of the DPIA. For instance, it does not mention when federal bodies are required to submit a DPIA to the FDPIC. In this respect, we would have welcomed, for example, a provision in the ordinance requiring the results of data protection impact assessments and the FDPIC's opinions on these to be indicated in the respective legislative dispatches to Parliament.

The FOJ plans to provide informal interpretative guidance. However, given the lack of detail provided by the legislator, businesses and federal bodies will have to rely largely on the wording of the law when it comes to fulfilling their data processing obligations. Without further clarification in the ordinance, in his capacity as a supervisory authority, the FDPIC will have broad discretion in applying the provisions of the law with a view to establishing a practice that guarantees both consistency and equality. However, by exercising the discretion afforded to him, he risks being accused of acting as a regulator.

The FDPIC also suggested amending the implementing provisions on administrative assistance, especially since the Federal Council has already acknowledged the problem of overlapping supervision by the FDPIC and foreign data protection authorities in its opinion of 9 November 2016 on the FDP's motion 16.3752 against an overlap in data protection.

Strengthening the role of data protection officers within the federal offices

In recent years, the FDPIC has given the data protection officers of private data processors increasing responsibility by considering them as primary contacts upstream of the official data protection supervisory authority for digitalisation projects in the private sector. The legislator also emphasises the increased importance of company data protection in the revised Federal Act on Data Protection. Practices that already produce good results in the private sector must be increasingly introduced in the Federal Administration if the FDPIC is to continue to fulfil his statutory duties under the new law with the resources at his disposal. In this context, the FDPIC demands that the current draft ordinance attach greater importance to the role of data protection officers within the federal bodies. In particular, we consider it imperative that the Federal Council introduce a new obligation to consult the data protection officers of the federal offices for the legislative projects of the Federal Administration.


Wenn Kategorien
zugewiesenen Cookies
jede zugeordnete Kategorie
Lernen Sie mehr
ALLE COOKIES ERLAUBEN
Notwendige Cookies
Notwendige Cookies
diese Cookies kann die
und können nicht deaktiviert
Benutzereinstellungen
Cookies ermöglichen es uns
und unsere website den
Dies kann das Speichern

NEW SERVICES

New online reporting portals

In order to implement the new Federal Act on Data Protection, the FDPIC will provide two new online reporting portals, which will be integrated into his own website.

- The first is a portal for reporting data security breaches and is intended to enable data controllers to fulfil their reporting obligation under Article 24 revFADP. The portal provides a fast and secure way to submit the necessary information to the FDPIC.

- The second is a reporting portal for data protection officers. It provides private data controllers and federal bodies with a simple way to submit the necessary information to the FDPIC. Under the revFADP, the designation of data protection officers is optional for private businesses and is a legal requirement only for federal bodies.

Furthermore, the existing portal for reporting and querying data collections, the so-called 'Webdatareg', will be completely overhauled. Unlike private data controllers, federal bodies are required to declare their records of data processing activities (formerly 'data files') to the FDPIC under the new FADP as well. The FDPIC publishes this data on his website.

DPCO

Revised Ordinance on Data Protection Certification

The complete revision of the Federal Act on Data Protection involved revising both the Ordinance on the Federal Act on Data Protection (OFADP) and the Ordinance on Data Protection Certification (DPCO). The FDPIC oversaw work on the draft DPCO, whereby certification has been extended to include services.

Previously limited to data processing systems (procedures and organisation) and products (programs and systems), the DPCO has been revised to extend certification to services.

This has been done to increase the transparency of data processing activities and reduce the risk of privacy breaches, thereby increasing trust in services. Certified data processors are exempt from the obligation to carry out a DPIA. Certification covers all aspects of data processing that would ordinarily need to be checked as part of a data protection impact assessment.

Article 6 of the revised DPCO now refers to ISO Standard 27701. This standard is an extension to ISO/IEC 27001 to include data protection and can only be certified in combination with ISO/IEC 27001. ISO/IEC 27001 establishes the requirements for information security management systems. The extension of the standard to include data protection requirements (ISO 27701) is intended to improve levels of data protection for services worldwide. ISO 27701 certification remains optional.

The FDPIC oversaw work on the DPCO from both a legal and an IT perspective. We were in contact with the Federal Office of Justice (FOJ) and other federal agencies such as the Swiss Accreditation Service (SAS) as well as private certification bodies.

The draft is not yet final at the time of going to press of the annual report. The above statements correspond to the status at the end of the reporting year. The FDPIC will further accompany the works.

ELECTRONIC IDENTITY

New State E-ID solution required

By rejecting the E-ID Act in 2021, Swiss voters have made it clear that they want digital identity management to be the sole responsibility of the State. The FDPIC aims to ensure that this new solution is also implemented in a privacy-compliant manner: it must provide a high level of security, user-friendliness and opportunities for individuals to exercise their self-determination.

After voters rejected the E-ID Act in the vote held on 7 March 2021, six identical motions from all parliamentary groups were submitted in the National Council calling for the creation of a new E-ID. The E-ID was to be a state-operated electronic means of identification to prove one's identity (authentication) online; The state authorities would be solely responsible for the issuing process and overall operation; The principles of data minimisation, privacy by design and decentralised data storage were to be observed.

Three solutions

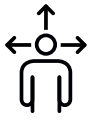
The motions were adopted, and the Federal Council instructed the FDJP (FOJ and fedpol) to work together with the FDF, the Federal Chancellery, the cantons and the Swiss Federal Institutes of Technology (ETH) to develop a new concept for an E-ID that met the requirements. The FDJP developed a basic concept based on three possible solutions for an E-ID or three different levels of ambition for an E-ID ecosystem:

a) an E-ID solution using a central governmental identity provider
b) an E-ID solution using public key infrastructure
c) an E-ID solution using self-sovereign identity.

The project managers kept the FDPIC up to date on the progress of the project. The FOJ also conducted an informal public consultation on the basic concept.

Anonymity in the public sphere

In this context, the FDPIC was invited to present his concerns regarding the discussion paper on the target vision for an E-ID at a public conference.



The FDPIC stressed that, regardless of the solution chosen, the E-ID had to allow individuals to continue to maintain anonymity when navigating the Internet. He also argued that individuals whose terminal was part of the infrastructure should be given the necessary support in pursuing decentralised solutions so that they could contribute to the security of the system without legal obligations being imposed.

After the Federal Council has made a policy decision on the design of the new E-ID, the FDJP will prepare the bill by mid-2022. The FDPIC will continue to voice his concerns in the ongoing project.

NEW RULES

Transparency of political funding

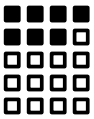
Following a popular initiative submitted in 2017, Parliament amended the Federal Act on Political Rights in 2021 to include rules designed to ensure transparency on political funding. The FDPIC is now focusing on the implementing ordinance, which is currently undergoing external consultation.

In autumn 2017, a popular initiative entitled 'For More Transparency in Political Funding' (Transparency Initiative) was submitted, and the Federal Council proposed rejecting it in August 2018. In 2019, the Council of States Institutions Committee drew up a report and put forward a counter-proposal to the initiative. In July 2021, the Swiss Parliament amended the Federal Law on Political Rights (PRA) and adopted rules designed to introduce transparency in political funding. Political parties will thus be obliged to publish information, mainly regarding donors, on significant donations, the amount of which will vary depending on whether they relate to an election or a voting campaign.

The Swiss Federal Audit Office (SFAO) – the authority responsible for carrying out the duties arising from the amendments to the PRA – contacted the FDPIC in connection with work on the implementing ordinance as both the Act and the ordinance deal with the publication of political data, i.e. potentially sensitive data if it can be traced back to a specific individual. In September 2021, the FDPIC met with the SFAO to exchange views and clarify a number of points.

FDPIC's requests

In November 2021, the draft ordinance was submitted to various federal offices for consultation. In this context, the FDPIC requested additional clarification of various points in the ordinance in order to ensure consistent application of the law and to provide a better framework for the processing of sensitive data. Therefore, as the SFAO has to publish the data as it receives it from the political movements, it has been clarified which documents are to be published and which are needed for audits. The aim was to prevent the publication of donors' personal information (e.g. their bank account details), which is irrelevant to providing transparency on political funding. Finally, the ordinance now specifies a five-year publication period.



The external consultation procedure took place from 17 December 2021 to 31 March 2022.


IC 8
12:16 Romanshorn
Winterthur Frauenfeld
SBB CFF FFS

KNOWLEDGE MANAGEMENT

Federal Administration know-how network based on AI

The FDPIC has been consulted by the Federal Office of Information Technology, Systems and Telecommunication (FOITT) about a planned pilot project for running a Federal Administration know-how network based on artificial intelligence (AI). Once the actual product has been purchased, an algorithm will be applied which, based on the digital evaluation of Federal Administration data files, will enable questions on specific topics to be directed internally to persons with the relevant expertise. In a first step, the FOITT is to conduct a data protection impact assessment.

Currently the Federal Administration uses traditional full-text search engines. These are neither able by themselves to link existing knowledge, nor do they usually provide context-related search results. They simply offer a word search, which returns results for one or more search terms from a limited content (e.g., a Sharepoint service). There is also no way to connect potential knowledge holders with these traditional tools.

In contrast to existing search functions or personal directories, the network being evaluated by the FOITT with the assistance of a private company is intended to identify and record the expertise available within the administration and make it available to all employees. Using the principles of artificial intelligence, an algorithm connects people with the relevant expertise to enable a rapid and appropriate response to questions and the sharing of experiences within the Federal Administration. To do this, the algorithm continuously creates increasingly detailed know-how profiles on the basis of questions and answers already fed in on specific topics. Based on these profiles, an automated process will then direct incoming questions to the appropriate employees. The algorithm should be able to answer questions that have already been answered, meaning that the machine answers need only be checked by human specialists.

In September 2021, at the FOITT's request, the FDPIC provided an initial written assessment of the general conditions required under data protection law in order to conduct a pilot project. In it, he advised the FOITT to conduct a data protection impact assessment (DPIA), which should identify the potential risks of the planned processing of personal data and propose measures to mitigate them. The further procedure and the plan for regulating a trial operation will then depend on the results of the impact assessment that the FOITT will begin in February 2022 and on the parallel clarifications on information protection and personnel law that it carries out.

1.2 Justice, Police, Security

COMPLETE REVISION OF THE CUSTOMS ACT

Creation of the Federal Office for Customs and Border Security

The FDPIC provided supervisory support in the legislative work of the Federal Office for Customs and Border Security (FOCBS) on the act on enforcement duties and in the development of a data protection impact assessment carried out in parallel. In the third office consultation, the FOCBS took on board the FDPIC's main recommendations for improvement.

On 11 September 2020 the Federal Council initiated a consultation on a legislative package referred to as the 'act on the enforcement duties of the FOCBS', aimed at establishing the legal framework for the digitalisation and transformation programme (DaziT) of the Federal Customs Administration (FCA). On 1 January 2022, the Federal Customs Administration was renamed Federal Office for Customs and Border Security (FOCBS).

The FDPIC provided supervisory support for the revision of the act and the development of a data protection impact assessment (DPIA) carried out in parallel. At our request, the FOCBS documented the changes introduced in the new act in terms of the scope and intensity of personal data processing. We also suggested that the FOCBS include systemic risks as well as security risks in the DPIA, namely the risks arising in connection with the creation of the new job profile of 'customs and border security specialist' (which combines the previous FCA occupations of customs specialist and border guard) and in connection with the development of a new application landscape in the form of a single information system.

After the third office consultation, the FDPIC noted significant improvements to the section on data processing (first consultation: see 27th Annual Report, section 2.4; second consultation: see 28th Annual Report, section 1.2). The FOCBS also took on board the FDPIC's main recommendations for improvement in relation to the DPIA. At the end of the year under review, it remained unclear to what extent the remaining differences could be resolved.

REVISION OF THE INTELLIGENCE SERVICE ACT

The revised Intelligence Service Act must guarantee the same level of transparency as the current IntelSA

In November 2020, the Federal Intelligence Service (FIS) informed the FDPIC that the Intelligence Service Act (IntelSA) was being revised to include new duties and a new data processing concept and to align the act with the new FADP. During the office consultation of summer 2021, the bill was improved significantly, and the FDPIC's demands were met. Differences of opinion remain regarding a mention of the information system. The consultation procedure is scheduled for spring 2022.

The IntelSA of 25 September 2015, which came into force on 1 September 2017 after a vote following a referendum, is now being completely revised to simplify data management in accordance with a mandate from the Delegation of Parliamentary Management Committees.

As part of the mandate, the section on data processing has been revised to introduce a paradigm shift from the existing multiple intelligence subsystems to a single system.

Over several stages of consultation, the FDPIC succeeded in having many of his demands regarding data processing provisions accepted. Therefore, the dispatch on the act will expressly state that the future processing of personal data must not differ substantially from the processing provided for by the law currently in force in terms of data categories and access rules. In the bill, these data categories have been established so that data processing can continue to be allocated to specific tasks of the FIS despite the subsystems being eliminated.

However, agreement could not be reached on a key point at the end of the year under review: the DDPS could not be persuaded to include in the bill that the FIS is required, in principle, to process all personal intelligence data using the above-mentioned single system in the future. The FDPIC noted that the processing of intelligence information by the former federal police in a multitude of non-transparent locations was a major point of concern raised in the report of the Parliamentary Investigation Committee of 22 November 1989 on the Secret Files Scandal.

By contrast, the expressed willingness to align the right to information under the IntelSA with the new FADP, thereby strengthening the rights of the individuals concerned, is to be welcomed.

It is also good that the plan – which we had criticised – to further restrict the scope of the Federal Act on Freedom of Information in the Administration (FoIA) as part of the revision has been abandoned.

The external consultation is due to begin in the second quarter of 2022.

RIGHT OF ACCESS

Applications for review in case of deferral

In the context of the right of access to certain personal data processed by the Federal Intelligence Service (FIS) and the Federal Office of Police (fedpol), the provision of information may be deferred without explanation. However, the applicant may ask the FDPIC to verify whether the processing of the data is lawful and whether the deferral is justified. The FDPIC processed 274 applications for review between 2018 and 2021.

When the FDPIC receives an application for review, he sends the applicant an acknowledgement of receipt. He also informs the office responsible for processing the data (FIS or fedpol) that he has received an application for review. The office concerned then informs the FDPIC as to whether or not the applicant is registered in its information systems.

If the applicant is not registered

If the applicant is not registered in its information systems, the office concerned informs the FDPIC via a "certificate of non-registration". The FDPIC then examines the application for

review. If the applicant makes a plausible argument that he or she would be seriously and irreparably harmed by deferral of a reply, the FDPIC informs the office in question that he intends to issue a recommendation (FIS) or a decision (fedpol), urging it to notify the applicant immediately that he or she is not registered. The office then has a chance to explain to the FDPIC why disclosure of the data to the data subject may pose a threat to internal or external security. If that is not the case, the office concerned informs the applicant that he or she is not registered. After that, the FDPIC sends the notification required by law. Always worded the same way, this notification informs the applicant that no data concerning him or her has been processed unlawfully or that the FDPIC has sent the office in question a recommendation (FIS) or a decision (fedpol) in order to remedy an error relating to the processing of their personal data or the deferral of its reply.

If the applicant is registered

If the applicant is registered in its information systems, the FDPIC sends two members of staff to visit the premises of the office in question to verify the lawfulness of the processing of the data held. After the review, the FDPIC determines whether or not the applicant makes a credible argument that deferral of a reply would seriously and irreparably harm him or her. If the FDPIC concludes that the processing of their personal data is unlawful, that the conditions for deferral are not met or that the conditions for immediate notification are met, he will inform the office in question that he intends to issue a recommendation (FIS) or a decision (fedpol). The office may then present its arguments. After the review, the FDPIC sends the notification required by law, which is identical in all respects to that sent to a non-registered applicant.

Some figures

Over the past four years (2018 – 2021), the FDPIC has processed 274 applications for review.

Most applications for review related to the Intelligence Service Act (180 applications): 8 in 2018, 42 in 2019, 107 in 2020 and 23 in 2021. Applications based on the Federal Act on the Federal Police Information Systems make up a smaller proportion (93 applications): 29 in 2018, 25 in 2019, 17 in 2020 and 22 in 2021. We received only one application for review under the Federal Act on International Mutual Assistance in Criminal Matters.

SCHENGEN INFORMATION SYSTEM

Coordination activities at national level

In the report year, the FDPIC was also involved in constant discussions with the European authorities and the cantons in order to work towards the uniform implementation of data protection provisions when using the various components of the Schengen Information System.

The SIS II Supervision Coordination Group has in recent years noted an increase in the number of alerts issued in the Schengen Information System (SIS) for discreet surveillance and specific checks on persons and vehicles in order to prevent threats and to safeguard internal or external security in the Schengen States (Article 36 of the EU SIS II Decision 2007/533/JHA) (see section 1.8). For this reason, it drew up a questionnaire for the various Schengen data protection authorities at national level. The FDPIC subsequently reviewed the legality of the processing carried out by the Federal Office of Police (fedpol), in particular the deletion of data in this connection,

and sent the completed questionnaire to the Secretariat of the SIS II Supervision Coordination Group. Based on his findings, the FDPIC concluded that there was no current need for action in fedpol's case in relation to this matter.

At video conferences held by the Swiss Schengen Coordination Group on 1 July and 2 December 2021, the FDPIC discussed the current developments in the Schengen field with representatives of the cantonal data protection authorities. The meetings focused on experiences with log file controls.

With a view to Switzerland's scheduled Schengen evaluation in 2023, a kick-off meeting was held in Bern with the participant authorities on 8 November 2021. The overall coordination of the Schengen evaluation is mainly carried out by the heads of the Swiss Delegation in the Schengen Committee. This comprises the Federal Office of Justice (FOJ), which has primary responsibility, and the jointly responsible Europe Division at the FDFA State Secretariat. The work is carried out by nine sub-working groups, with the FDPIC participating in the data protection sub-working group. The questionnaire should be sent to the participant authorities in the first half of 2022. They will be given eight weeks to respond, after which their answers will be analysed. The European experts are planning to visit Switzerland at the start of 2023.

1.3 Commerce and economy

DIGITAL CURRENCY DIEM

Diem abandons plans for blockchain payment system in Switzerland

In spring 2021, the Diem Association (formerly Libra Association) withdrew its application to the Swiss Financial Market Supervisory Authority (FINMA) for authorisation as a blockchain-based payment system in Switzerland. The FDPIC therefore ended his supervisory and advisory activities in connection with the project, which he had started in 2019.

The Geneva-based Diem Association (Diem) is a membership-based association dedicated to building a blockchain-based payment system. The FDPIC contacted Diem (then Libra Association) for the first time in July 2019 after learning about its project. From that point on, he was in regular contact with the project managers at Diem and representatives of a number of national and international supervisory bodies (see 27th Annual Report, Focus II).

In spring 2021, at the FDPIC's request, Diem submitted various documents relevant to data protection, namely drafts of a data protection concept and a risk impact assessment. The FDPIC intended to carry out technical and data protection assessments of the project based on the information received.

In May 2021, while our analyses were underway, Diem announced a strategic relocation of its primary operations from Switzerland to the United States. At that time, Diem planned to launch its payment system from the US in the first phase. In addition, it planned to make the payment system available initially only to US financial service providers.

As a result, Diem withdrew its application to FINMA for authorisation of the payment system in Switzerland, which was already well underway. As the FDPIC was no longer responsible for the matter, he brought his investigation to a close. According to media reports, however, the project is about to fall through in the US as well.

SEC SUPERVISORY PROCEDURE

The transfer of data to the US Securities and Exchange Commission is permitted in principle.

At the request of the US Securities and Exchange Commission (SEC), the FDPIC has clarified whether or not Swiss companies that registered with the SEC were permitted to provide the SEC with the data required under US law in the course of an SEC supervisory procedure without violating Swiss data protection law. In principle, they are permitted to do so. The FDPIC has drawn up a memorandum on the subject. The question regarding the transfer of personal data protected under criminal law remains open.

During the year under review, the US Securities and Exchange Commission (SEC) contacted the FDPIC requesting clarification as to whether or not Swiss companies that registered with the SEC were permitted to provide the SEC with the personal data required under US law in the course of an SEC supervisory procedure without violating the Swiss Federal Act on Data Protection (FADP). Up until now, the SEC has not allowed Swiss companies to register for fear of not being able to obtain the necessary data in the event of a supervisory procedure.

After obtaining the necessary documentation, the FDPIC drew up a memorandum on the subject, in which he concluded as follows: In the absence of an adequate level of data protection

in the US, Swiss companies may disclose personal data to the SEC only if one of the justifying grounds for cross-border disclosure set out in Article 6 para. 2 FADP is met. Data disclosure to the SEC may be justified on a number of the grounds listed.

The disclosure of data to the SEC is regularly justified on the grounds that the processing is directly connected with the conclusion or performance of a contract (Art. 6 para. 2 let. c FADP). However, other grounds for justification of data disclosure include the safeguarding of an overriding public interest (Art. 6 para. 2 let. d FADP) and the data subject having consented (Art. 6 para. 2 let. b FADP).

The FDPIC has expressly left open the question as to whether – and, if so, under which conditions – personal data that is protected under both the FADP and criminal law (particularly information subject to banking secrecy) may be disclosed to the SEC. The FDPIC is not competent to interpret the Swiss Criminal Code or any other relevant laws. The memorandum can be found on the FDPIC's website. The SEC has not provided us with any details regarding the consequences in terms of allowing Swiss companies to register.

ONLINE STORE

Processing of customer data

During the year under review, the FDPIC resolved open questions and unclear issues regarding customer data analysis as part of a case investigation carried out at one of Switzerland's largest online store.

In spring 2021, the FDPIC had initiated a procedure at one of Switzerland's largest online store to assess the privacy compliance of its customer data processing. Our investigation focussed, among other things, on the online store operator's handling of objection requests from customers.

After a preliminary investigation, in which we were able to establish that the operator rejected objections to certain types of data processing – particularly regarding the recording and analysis of purchasing behaviour in a way that allows the data subjects to be identified – we wanted to find out whether the data processing in question could take place against the express will of the data subjects (see 28th Annual Report 2020/2021, section 1.4).

During the year under review, the FDPIC reviewed the store's data processing activities and questioned the operator on them. On 26 January 2022, he was able to establish the facts and start his legal analysis. The analysis was ongoing at the time of writing this report.

SWISS MARKETPLACE GROUP

Auction platform Ricardo: New developments in the procedure

During the year under review, there were further significant developments in the procedure initiated in 2017 against Ricardo and the TX Group regarding the use of data collected by the online auction platform ricardo.ch.

Since 2017, we have reported annually on developments in the case investigation into Ricardo and the TX Group. According to our legal assessment, data subjects must be clearly informed of the profiling activities carried out by TX Group for the purpose of targeted advertising using data from a number of different sources. Furthermore, the express consent of the data subjects is required in this case (see 28th Annual Report 2020/2021, Section 1.4).

Meanwhile, significant changes and adjustments have been made to the platforms of both Ricardo and the TX Group. In this regard, we investi-

gated the new Consent Management Platforms (CMP) in particular. We also reviewed the legitimate interest assessment submitted to us in August 2021, in which the TX Group states that it has an overriding private interest in the use of Ricardo data and in cross-platform profiling for the Group's targeted advertising and that data subject consent is therefore not required.

At the end of November 2021, the TX Group also informed us that the companies TX Group AG, Ringier AG, die Mobiliar AG and General Atlantic had formed a joint venture with the Swiss Marketplace Group (SMG) on 11 November 2021. The SMG now comprises various digital marketplaces, including Ricardo AG with its portals and offerings. The FDPIC is now investigating the impact of these technical and organisational changes on the data processing activities investigated in this procedure. The investigation was still ongoing at the time of going to press.

CREDIT CHECKS

Investigations into a vehicle-leasing provider

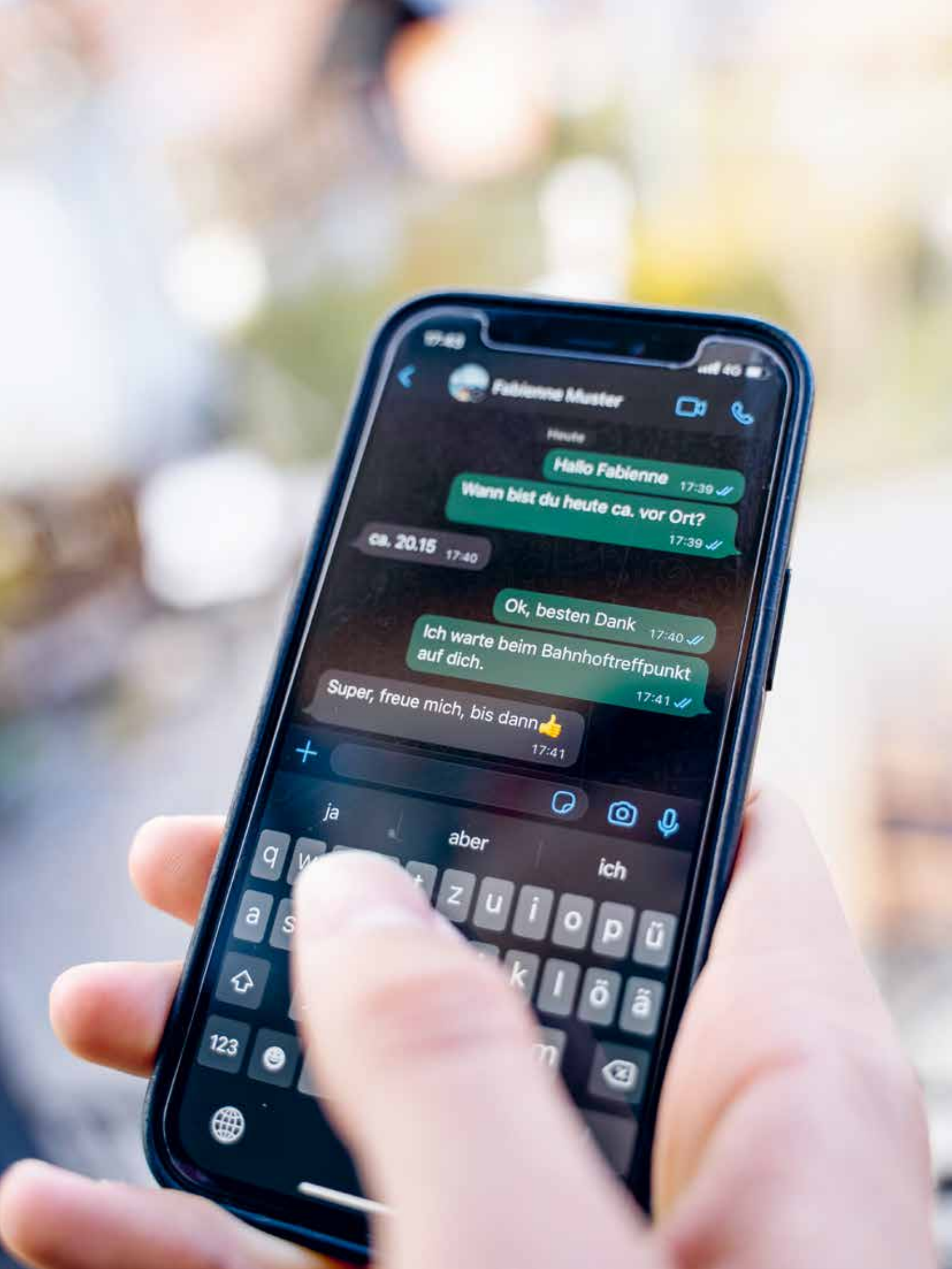
The FDPIC successfully concluded investigations begun in the previous report year into a major vehicle-leasing provider in relation to data processing when checking the creditworthiness of customers. No formal measures were taken. The leasing provider has given an assurance that it will implement two proposals made by the FDPIC on improvements relating to consent.

In order to enter into a leasing contract for a car, customers must consent to the leasing provider checking their creditworthiness. As a result of enquiries from members of the public, the FDPIC learned that one leasing provider requests applicants to consent to it obtaining a range of information from third parties in order to check their creditworthiness. The customers concerned must also agree to allow information to be obtained on third parties, such as their husband/wife or other family members.

The Commissioner therefore began preliminary enquiries at the leasing provider in December 2020 in order to confirm whether the data processing falls within the limits permitted under data protection law (see 28th AN, Chapter 1.4). After evaluating the statement from the leasing provider, the FDPIC concluded that the data processing described that is required to clarify the solvency and creditworthiness of leasing applicants is likely to be largely in line with the requirements under data protection law.

However, the Commissioner expressed certain reservations, firstly with regard to processing data relating to applicants' partners who live in the same household. He recommended that where the leasing provider processes data about an applicant's partner, it should obtain the partner's signature or declaration of consent in confirmation.

Secondly, he objected to the ostensibly irrevocable opening of data locks at debt enforcement offices, the ZEK, IKO and Swiss Post. The FDPIC pointed out to the leasing company that consent to data processing may be revoked at any time, and the revocation requires no specific form or justification. This is why a clause in the consent form to the effect that any data locks are 'irrevocably' opened has to be removed. The leasing company gave assurances that it would implement both measures.


Fabienne Muster
Heute
Hallo Fabienne 17:39
Wann bist du heute ca. vor Ort? 17:39
ca. 20.15 17:40
Ok, besten Dank 17:40
Ich warte beim Bahnhoftreffpunkt auf dich. 17:41
Super, freue mich, bis dann 17:41
ja
aber
ich

MITTO AG

Investigation into possible abuse of access to signalling system

In a report published in the media on 6 December 2021, serious allegations were made against an employee of the Zug-based company Mitto AG. The company is said to provide text messaging services to various large companies worldwide, enabling third parties to carry out unauthorised surveillance of individuals in return for payment.

The Bureau of Investigative Journalism, a non-profit organisation in London, and Bloomberg News published a report in which an employee of the Zug-based company Mitto AG is alleged to have abused the access granted by the mobile operators to their networks for the purpose of sending text messages in order to obtain information. According to the report, the person in question allegedly used the Signalling System (SS7) access in particular to enable third parties to carry out unauthorised surveillance of individuals in return for payment.

The FDPIC opened a preliminary investigation into the matter on 7 December 2021. As a first step, he asked Mitto AG to comment and also contacted the mobile network operators in Switzerland. The latter confirmed that they cooperate with Mitto AG but pointed out that sufficient technical safeguards were in place to prevent unauthorised access to personal data. On the basis of this initial feedback, the FDPIC has no indications for the time being that any misconduct has occurred to the detriment of people in Switzerland.

Mitto AG informed the FDPIC that it had no knowledge of any such incident. At the FDPIC's request, the company provided documentation on the technical and organisational measures implemented to protect personal data. The FDPIC is examining the documentation to identify any shortcomings at Mitto AG regarding control mechanisms and the assignment of access rights to employees. The investigation was still ongoing at the time of going to press.

SOCIAL MEDIA

Growing interest in privacy after WhatsApp updates its terms of service

In January 2021, instant messaging service WhatsApp announced that it was updating its terms of service and privacy policy, stating that users needed to accept the new terms to continue using the service. The FDPIC examined the changes in question and answered questions from concerned members of the public and the media.

It is often said that most people are readily willing to give up their personal data in exchange for a free service. However, when WhatsApp announced its new terms of service, that was not the case. After WhatsApp's announcement, worried members of the public contacted the FDPIC with their concerns. They were reluctant to accept the new terms for fear of losing control over their own data. At the same time, they realised that they depended on the service as their families and friends were unwilling to switch to alternative services. As a result, the FDPIC took a

closer look at the changes to WhatsApp's terms of service and privacy policy.

He found that the uncertainty among WhatsApp users probably stemmed from the fact that there were now two different versions of the terms of service and privacy policy: one for Europe (including Switzerland) and one for the rest of the world. He noted major changes to the latter. For example, the Meta Group (formerly Facebook Inc.) now reserves the right to link the data from its various services (WhatsApp, Instagram and Facebook) even more closely and also to use it for marketing purposes or share it with third-party companies. This relates only to the metadata and not to the content of messages or calls, which remains encrypted end-to-end and is thus unusable. However, compiling and analysing this data allows Meta to draw various conclusions about users such as how frequently they interact with a group or another person or what their interests are based on the groups they have joined etc.

Hardly any changes for users in Switzerland

However, the FDPIC's investigations revealed that the new terms of service for users in Europe (including Switzerland) had hardly changed in terms of content. Most of the changes were language-related, either providing clarification (e.g. information on metadata of messages or cooperation with other Meta companies) or additions (e.g. regarding the legal basis of data processing, the handling of users who violate the terms of service or policy, or the data stored). The only completely new content were the provisions specifying which data could be processed in the future when a private individual contacts a company via WhatsApp using the newly introduced business accounts. However, there are no changes for users who do not use WhatsApp business accounts. The FDPIC announced this in response to public and media enquiries.

Even though most of the fears of Swiss users proved unfounded, the discussions about WhatsApp's new terms of service led many members of the public to reconsider their use of free services. The discussions raised awareness of the fact that many of these offers are based on business models that rely on data monetisation and that it is therefore worth reading the terms and conditions and privacy statements more carefully. However, we recommend this not only in connection with the use of free services but whenever entering into an agreement with a service provider, regardless of the price model, as customer data may be processed for the service provider's own purposes even with paid services.

The FDPIC notes that terms and conditions and privacy policies that are set out in detail but are difficult to understand for the layperson can hardly be regarded as providing additional transparency. In this regard, as part of his advisory and supervisory activities, he is working to improve the quality of the information provided to users.

ONELOG

Swiss media publishers join forces to create a single sign-on system for online portals

During the year under review, the FDPIC continued to follow the progress of the Swiss publishing houses' project aimed at creating a single sign-on system for online media portals.

Swiss publishing houses continued work on a single sign-on system for the media portals they operate (see 28th Annual Report, section 1.1). The media publishers involved in the project founded the company OneLog, a joint venture that centrally operates the single sign-on solution (SSO), acting mainly as a data processor under contract.

The FDPIC's suggestions for improvement were taken on board and the corresponding technical and organisational measures were implemented. These prevent the media publishers from being able to exchange and link personal data via OneLog in order to

obtain information about users that has been collected by other media publishers.

Furthermore, OneLog has put in place rules and processes to ensure privacy compliance and to enable users to exercise their rights, particularly their rights to access, delete and correct their personal data. Participating media publishers are required to sign a contract with OneLog under which they are duty bound to use the SSO system in a privacy-compliant manner. OneLog has also appointed an operational data protection officer to monitor compliance with data protection regulations throughout the system.

The SSO system went live in late summer of the reporting year, since which time the sign-on process for a number of media portals has been managed by OneLog. We shall continue to monitor the project's progress.

POSTFINANCE

Automatic entry of account details

The FDPIC was alerted by a member of the public to the fact that the PostFinance e-banking portal provided access to the details of any number of post office account holders. Since then, the post office has introduced technical measures to limit the automatic entry of account details to a reasonable number of queries. In addition, the FDPIC demands that customers be given an opportunity to object to their details being made publicly accessible.

As long as Swiss residents made most of their payments in cash at the post office counter, the correctness of the recipients' details were checked manually: There was a publicly accessible directory listing all post office account holders along with their names and addresses. A few years ago, this directory of account details was integrated into PostFinance's e-banking system so that when a user entered a PostFinance account number in the payment entry form, the system would automatically enter the account holder's name and address. Today, this function is still available and serves to ensure secure, trouble-free payment transactions by minimising data entry errors. It is limited to PostFinance accounts, and customers are informed about their account details being made publicly accessible in the terms and conditions and in a separate leaflet.

However, according to the report we received, PostFinance's e-banking portal allowed users to enter an unlimited number of account numbers. This meant that any number of account numbers could be checked in succession, allowing bulk queries to be performed

on account holders. When we contacted PostFinance, it confirmed to us that the query limit originally set had been inadvertently deactivated, as a result of which bulk queries were possible for about two years. After the member of the public also contacted PostFinance directly, the query limit was reactivated, allowing no more than 10 queries in a 24-hour period.

The FDPIC concluded that the automated entry of post office account holder details served a reasonable purpose and that PostFinance customers were adequately informed about this. Furthermore, the risk of bulk queries had been reduced to a reasonable level with the reactivation of the query limit.

However, given that the function is not absolutely necessary for the processing of payment transactions and ultimately relies on data subjects' consent, customers should be given the opportunity to object to such use of their data. Therefore, the FDPIC has asked PostFinance to introduce an opt-out system.

CREDIT CHECKS

Incorrect database records kept by debt collection companies

In the ongoing investigation into allegedly incorrect database records at one of Switzerland's leading for debt collection and credit rating companies, the FDPIC has obtained further information on the issue of 'negative household results'.

As mentioned in our previous annual reports, in February 2020 the FDPIC opened an investigation into a major provider of debt collection and credit rating services based on allegations of incorrect database records leading to the data on people with the same or similar names and addresses becoming confused. It was also suggested that it may be difficult to correct these incorrect records (see 27th AR, Chapter 1.4).

In a second stage, the FDPIC expanded the investigation in response to questions from members of the public and from the media to include the issue of 'negative household results'. By this is meant cases where a credit check on one household member results in negative credit-rating information on other persons in the same household being disclosed (see 28th AR, Chapter 1.4). This type of disclosure of personal data to online traders is intended to prevent persons with negative credit ratings

from being able to make a purchase on account by using the name of a member of the same household who has a positive credit rating, thus circumventing the credit-rating system. The practice of negative household results raises data protection-related questions, which is why the FDPIC obtained additional information from the company. An evaluation of the legal aspects of this information is ongoing. Based on the results, the FDPIC will decide on whether further action is required.

CLUBS AND ASSOCIATIONS

Shooters issued with new membership card that doubles as a credit card

The Swiss Shooting Sport Federation (SSV) has issued a new membership card that doubles as a credit card to more than 50,000 licensed shooters. Many federation members have voiced their discontent over the commercial use of their details. The FDPIC has worked with the SSV to achieve data protection-compliant handling of members' personal data.

The issue of more than 50,000 new membership cards that double as credit cards has raised concern among many federation members over the protection of their data. As a first step, the FDPIC obtained more information from the Federation on how the data was used.

Although the Federation had already outsourced the issuing of membership cards to an external company in the past, the newly selected credit card provider was also pursuing its own goals with the order received, thus gaining access to new customers. The transfer of members' data to the credit card provider constitutes data disclosure and must therefore comply with the data processing principles set out in the Federal Act on Data Protection with particular regard to that of purpose and the obligation of transparency.

Personal data may only be processed for the purpose specified at the time of collection, as indicated by the circumstances or as provided for by law. Since 2016, the SSV's Articles of Association have provided for disclosure of members' data for commercial purposes, offering members an opt-out option. In so doing, the SSV has essentially laid the groundwork for the commercial use of its members' data.

However, the problem is that the provision in question is expressly mentioned only in the Federation's Articles of Association. The articles of association of the 36 affiliated associations and more than 2000 clubs typically lack a similar provision and include only a general reference to the SSV's Articles of Association. Consequently, individual members of the various associations had considerable difficulty finding out about this provision and exercising their right to object. The FDPIC stated that the SSV's disclosure of data to the credit card provider failed to meet the obligation of transparency under data protection law. Under this obligation, data subjects are to be clearly informed of the purpose for which their personal data will be processed.

In consultation with the SVV, it was agreed that the Federation could inform shooters once again via its website, newsletter and members' magazine about the disclosure of their personal data for commercial purposes, informing them of their right to object to such use by simply notifying the Federation.

The SSV will then need to check to ensure that the credit card provider is

treating separately the personal data of members who only want a simple membership card (without the credit card feature) and that it does not use their details for its own purposes such as marketing or submitting offers. Members who have opted not to receive a membership card in the form of a credit card can continue to identify themselves at events by showing an ID document along with their membership number.

1.4 Health

CORONA

Advising on the project for a data protection compliant COVID-19 certificate and the 'Certificate Light'

The FDPIC attended the meetings of the project group set up by the Federal Office of Public Health to develop a standard, forgery-proof, internationally recognised COVID-19 certificate. He provided advice and insisted on the creation of the 'Certificate Light', which contains a limited amount of data.

As a measure to contain the COVID-19 pandemic, Switzerland introduced the COVID-19-certificate in the early summer of 2021 as proof of vaccination against the Sars-CoV2 virus, recovery from infection or a recent negative test. The basis for the certificate lay in Article 6a of the COVID-19 Act. As part of his statutory duty to advise the project group set up by the Federal Office of Public Health (FOPH), the FDPIC called for the legislative mandate to be carried out in accordance with data protection requirements. This meant that the certificate had to be personal, forgery-proof, verifiable in compliance with data protection law and designed so that its authenticity and validity could be checked on the spot through a decentralised system. In this way, the certificate can be used when entering or leaving other countries. In addition, from the outset the FDPIC demanded that the introduction of the certificate should not lead to a general obligation to carry smartphones. By allowing the COVID-19 certificate to be used in both digital and paper form, this concern has been taken into account.

Limited-data Certificate Light

The FDPIC also successfully insisted that the Federal Office of Information Technology, Systems and Telecommunication (FOITT) develop a second, data-light QR code for use in Switzerland, the 'Certificate Light', alongside the EU-compatible certificate for cross-border travel. The QR code can be generated in the app and contains no information on whether the certificate is based on a test, a vaccination or recovery from the illness. To ensure that no conclusions can be drawn about the basis on which it is issued, the Certificate Light is only valid for a short period and must then be regenerated. It is only valid in Switzerland.

The Certificate Light therefore only contains the details required to identify the holder and an electronic signature. This also eliminates the risk that a checking-app other than that provided by the Confederation can unlawfully read health-related data from the certificate. It is normally not necessary when conducting entry checks at an event for information to be disclosed on whether the holder of a certificate has obtained it based on a vaccination, recovery from the illness or a test.

Problems caused by the 2G regime

The spread of the pandemic caused the Federal Council in December 2021 to limit access to certain establishments and events to people who could prove that they had been vaccinated or had recovered from COVID. This meant that a negative test result was no longer sufficient to gain entry. Under this regime, known as '2G' or '2G+', the Certificate Light could no longer be used at first, as by design this certificate gives no indication of the holder's

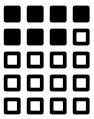

13:31
COVID-ZERTIFIKAT

health status (vaccinated, recovered or tested negative). This limitation was neither planned nor foreseeable when the certificate system was conceived. In order to be able to use the Certificate Light under the 2G regime, or if need be other parallel arrangements depending on the situation, either different forms of the Certificate Light would have to be issued (2G+, 2G and 3G) or information on the type of authorisation would have to be stored directly in the Certificate Light. The latter would mean adding health information to the Certificate Light – which would be contrary to its original purpose. Regardless of what solution was eventually chosen, the FDPIC demanded that the Certificate Light be able to be used again with its full functionality if the 3G regime returns.

Proportionate use of the certificate

In addition to advising on the data protection compliant design and future technical development of the certificate, the FDPIC continued to work to ensure that the way in which the certificate is used is not simply left to the discretion of the private individuals concerned but is governed by a public-law framework of rules.

The requirements for using the certificate are set out in the Ordinance on Measures during the Special Situation to combat the COVID-19 Epidemic (COVID-19 Special Situation Ordinance; SR 818.101.26). Although the certificate requirement was initially conceived solely for large-scale events, as the pandemic progressed use of the certificate was gradually expanded to include other sectors, including restaurants and bars and leisure facilities such as museums, libraries, zoos, gyms, indoor swimming pools and casinos. The FDPIC repeatedly noted in the course of several consultation procedures, often conducted at very short notice, that entry restrictions based on a certificate and the associated processing of health-related data can only be considered proportionate from a data protection standpoint if these measures are necessary and appropriate for combating the pandemic from an epidemiological perspective. Providing this evidence is the responsibility of the Federal Office of Public Health, and the FDPIC has always been guided by its findings and assessments.



In particular, faced with the possibility of extending the certificate requirement to workplaces, the FDPIC took the position that employers may only demand that employees provide a certificate within the scope of their duty of care after a careful weighing of interests and exclusively in connection with organising specific protective measures or implementing a testing plan.

CONTACT TRACING

Case investigation into the SocialPass application

As part of a case investigation, the FDPIC examined the private SocialPass application used to collect contact details at restaurants and other venues. In his final report, he recommended, in particular, that the app's operators improve the technical security of the application and grant the cantonal health authorities limited and proportionate access to query centrally collected data. Initially disputed, the FDPIC's key recommendations have since been accepted and largely implemented.

In summer 2020, in an effort to combat the pandemic, restaurants and venues were obliged to collect the contact details of all guests and attendees so that they could forward this information to the cantonal health authorities for the purpose of contact tracing in the event of a confirmed case of COVID-19 infection.

Jointly operated by two private companies based in Switzerland, the SocialPass app provided an easy way to collect this information using a Smartphone. However, the application raised a number of privacy concerns among the public, as a result of which the FDPIC opened a formal procedure in December 2020 to investigate the allegations, which were also widely reported in the media. In his final report, the FDPIC identified several shortcomings, for which he issued the app's operators with ten recommendations, the majority of which they accepted after several video conferences attended, among others, by the health authorities of the cantons of Vaud and Valais.

The FDPIC's key recommendations and their implementation

As well as identifying technical and organisational shortcomings, the investigation revealed that the private operators had granted the health authorities of the cantons of Vaud and Valais direct access to the central database, making it available for virtually any person-related queries without the need for any justification, thereby violating the principle of proportionality. According to media reports, the access granted to the canton of Valais even resulted in improper processing of personal data. The operators acted on the FDPIC's recommendation and eventually acknowledged the initially disputed shortcomings, reporting that these had since been rectified.

Unusually long and drawn-out procedure

The private SocialPass application was used across Switzerland to process personal information for the purpose of fighting the pandemic. In this context, the FDPIC had to keep a close eye on epidemiological developments in order to complete his investigation in good time. However, the procedure was unusually long and drawn out. When setting response times and handling the numerous applications for extension and even for rejection of the

FDPIC employees entrusted with the dossier, the FDPIC had to take into account the fact that the second wave of the pandemic was levelling off towards the beginning of summer 2021. As a result, restaurants were due to reopen shortly, and therefore the SocialPass app was about to be used again.

The easing of restrictions meant that the FDPIC had to inform the public in good time about the technical capabilities of the SocialPass app and the privacy risks associated with its use. Therefore, on 31 May 2021 – the day on which restaurants resumed service indoors – the FDPIC issued a press release in which he announced the main focus of his investigation and his findings up until that point along with his key recommendations.

The investigation into the SocialPass app proved necessary and useful and provided the FDPIC with an opportunity to comment on the division of supervisory duties between the federal and cantonal authorities as well as other privacy issues, which, because of their fundamental importance, could also be applied in part to other applications used by private individuals and authorities for the purpose of contact tracing.

MYVACCINES.CH

Investigation into myvaccines.ch

After the online magazine Republik uncovered serious data protection failures on the myvaccines.ch platform in March 2021, the FDPIC opened a formal procedure against the platform's operator just before publication. The failings identified made it impossible for the platform to continue to operate, and the foundation – partly financed by the FOPH – eventually filed for bankruptcy. The FDPIC supported the FOPH in order to allow users to access their data again.

In spring 2021, the online magazine Republik highlighted serious data protection and security failures on the online platform myvaccines.ch. The Myvaccines foundation, which operated the platform, was financed, among others, by the Federal Office of Public Health (FOPH), which promoted the platform on its own website and in brochures as an "electronic vaccination record".

After summarily assessing the plausibility of the allegations, the FDPIC opened a case investigation into the platform on which users recorded their vaccinations just before the allegations were published. An audit later conducted by the Foundation found that the failings exposed by the online magazine could not be readily remedied, and so the Foundation took the platform down for the time being.

At the end of July 2021, the FDPIC submitted his final report to the Foundation. In his report, he issued three recommendations relating in particular to the potentially compromised integrity of the data and its fate in the event of the platform being shut down. In particular, the Foundation could not rule out the possibility that unauthorised access may already have taken place and that the data may have been altered in the process.

The Foundation accepted the FDPIC's recommendations and

announced shortly after completion of the investigation that it would shut down all its activities and file for bankruptcy. From that point on, the Foundation no longer processed users' requests for

information or deletion of data. Consequently, the FDPIC received a steady stream of enquiries from those affected.

In an effort to give data subjects access to their data despite the online platform shutting down and the operator's impending liquidation, the FDPIC held numerous meetings with the FOPH as part of the project aimed at saving the data ("Datenrettung meineimpfungen"), during which he provided advice and specified the data protection requirements for sending vaccination data to users. Given the limited financial means available and the failings identified in the investigation, it was clear that certain compromises on privacy had to be accepted in order to find a practical solution that could be implemented in the short term.

In November 2021, the Foundation began sending users their vaccination records unencrypted by email without prior notice. Contrary to the Foundation's public statements, this procedure was not cleared by the FDPIC: on the contrary, it went against the recommendations issued by the FDPIC in his final report of 31 August 2021 as well as the requirements for data protection-compliant transmission of personal data presented to the FOPH. After the FDPIC intervened, the Foundation stopped sending data. Shortly afterwards, the Foundation was declared bankrupt. The FDPIC is considering filing a criminal complaint. The necessary investigations were still ongoing at the end of the reporting year.

The FDPIC now urges the FOPH to assume its responsibility despite the ongoing bankruptcy proceedings and to continue working to develop a privacy-compliant solution capable of giving data subjects access to their vaccination records in a way that best protects their privacy.

PATIENT RECORDS

Data storage, access and deletion

A regularly recurring theme in the FDPIC's advisory activities is the handling of patient records, in particular questions as to whether and when patients may demand that their medical history be handed over or deleted and how long doctors are required – or indeed allowed – to retain their records. Furthermore, a recent change to the Statute of Limitations Act also has implications for the retention of medical records.

The FDPIC received frequent enquiries again this past reporting year regarding the handling of patient records, confirming a high level of public interest in and uncertainty about the issue. Patient records – often referred to as "medical history" – include records

that arise in connection with medical treatment, such as reports, x-rays, laboratory results and correspondence with other healthcare providers. Under data protection law, patients are entitled to access their medical records. In practice, this right is regularly exercised.

However, the right to request the deletion of one's data – also provided for in data protection law – conflicts with record-keeping obligations imposed on medical professionals by cantonal health laws, for example. Therefore, physicians are generally unable to comply with a patient's request to delete all their information or to hand over all original documents to them as this would amount to a breach of their record-keeping obligations.

The Federal Act on Data Protection provides only an indirect answer to the question of how long physicians may or are required to store their patients' medical records. In accordance with the principle of proportionality, healthcare professionals may keep patient records for as long as they are needed. After completion of a course of treatment, the information may need to be retained for a longer period of time, for example for the purpose of providing evidence, namely until expiry of the time limit for the submission of any claims arising from the treatment in question, or if legal proceedings are likely. Therefore, as a general rule, the general limitation periods provided for in the Code of Obligations are usually taken into account.

These provisions were amended with effect from 1 January 2020: the limitation period for personal injury claims has been increased from 10 to 20 years. Some cantonal health laws that regulate the record-keeping obligations of physicians have already been amended accordingly and now also specify a longer retention period, with implications for the retention of patient records. This means a retention period of 20 years.

Treatment at hospitals with a cantonal service mandate is typically subject to cantonal law and the retention obligations and periods provided for therein.

Electronic patient records under the EPRA

Even though medical records are increasingly being managed electronically, they are generally not (yet) electronic patient records within the meaning of the Swiss Federal Act on the Electronic Patient Record (EPRA). There has been a significant delay in the introduction of this form of patient-centred documentation, partly as a result of the pandemic. However, the year under review saw an increase in the number of certified reference communities, i. e. communities that service providers such as doctors, therapists and hospitals can join in order to offer their patients electronic patient records. The first electronic patient records are due to be rolled out in May 2021.

In parallel with the introduction of EPRs, there have been calls, notably from political circles, for changes to the EPRs aimed at further promoting their use. The FDPIC is following the relevant initiatives and developments and is in regular contact with the FOPH, the cantons and other actors.

SECURITY OF REGISTERS

Vulnerability of organ donor and breast implant registers

It seems that not enough attention has been paid to data protection in the management of registers in the healthcare sector. During the first quarter of 2022, the FDPIC intervened in a number of problematic cases reported by the media.

Since the beginning of 2022, the media have drawn attention to two registers in particular, highlighting serious data protection failings.

The first case concerned the national organ donor register, set up and managed by the Swisstransplant foundation, and specifically the accuracy of the data entered. It was discovered that anyone could enter a third party in the register, specifying their alleged consent or objection to organ donation, without the person's knowledge. After checking the plausibility of the facts brought to his attention and taking immediate action to limit the damage, the FDPIC opened an investigation into the matter (Art. 29 FADP), during which the identification processes will be assessed and improved.

There is also a political component to this case in view of the referendum on 15 May 2022. Swiss voters will be called upon to decide on a change to the organ donation system. As things stand, a person has to give explicit consent for their organs to be used after their death. The proposed change reverses the current opt-in policy, introducing the concept of presumed consent, meaning that organs may be removed unless the deceased explicitly objected. The new system would require the creation of a new register, in which individuals could register their preference; it should be noted that the new register would be different from the existing one although it would serve the same purpose.

The second case concerned the breast implant register managed by Swiss Plastic Surgery. The register contained IT security gaps and design errors, making it relatively easy for unauthorised persons to gain extensive access to patient data. In this case, too, the FDPIC checked the plausibility of the facts reported and took measures to reduce the damage. The FDPIC is currently evaluating further action.

In general, these two recent cases and the case of the Myvaccines foundation (see article above) show that the security of registers managed by private associations and foundations – which sometimes also process personal data on behalf of the health authorities – is often neglected. The FDPIC stresses that when operators create a register, it goes without saying that they need to be fully aware of their responsibility in terms of data security and accuracy. Therefore, a comprehensive data management concept is essential from the moment data is collected to the moment it is destroyed. This requires adequate IT organisation, staff organisation and access management. With regard to the data subjects' information, in the absence of any justification, which the person responsible for managing the register could use, data subjects must be clearly informed about the ways in which their data will be used before giving their consent.

CYBER ATTACKS

Patient records published on the dark web

In March 2022, media outlets in the French-speaking part of Switzerland reported that a large amount of health data had been published on the dark web. The FDPIC demanded that the medical practices fully inform patients about the incident. The medical practices affected in the French-speaking part of Switzerland have already taken initial measures to rectify the data protection and security deficits.

This cyber attack is further proof that particularly sensitive health data is insufficiently protected in Switzerland. The FDPIC hopes that the medical profession and industry representatives recognise the urgent need for action.

1.5 Employment

FEDERAL EMPLOYEES

Enquiry at the Swiss Federal Statistical Office into the retention of physical personnel records

The FDPIC has conducted an investigation at the Swiss Federal Statistical Office (FSO) into the way in which physical personnel records of former employees are dealt with. It revealed that there is a need for action. The Swiss Federal Statistical Office has recognised this and submitted a proposal to the FDPIC on how to comply with the law in future.

The law applicable to federal employees stipulates, that personnel records are retained for ten years after an employee has left their position in the Administration. At the end of this period, the records should be offered to the Federal Archives for safekeeping. The data that the Federal Archives regards as not worth archiving should be destroyed. Following an enquiry from a member of the public, it came to the FDPIC's attention that the Swiss Federal Statistical Office (FSO) may have been retaining a large number of personnel records pertaining to former employees for longer than the law permits. In response, the FDPIC conducted an initial investigation at the FSO.

Enquiries revealed that the system for retaining physical personnel records of former employees did not meet the statutory requirements. For a long time, the FSO has not been destroying the personnel records of former employees after ten years, but continuing to store them. The FSO has recognised the need for action and at the request of the FDPIC submitted a plan and schedule for restoring compliance with the law. This provides for the required work to be completed by the summer of 2022. In the circumstances, the FDPIC decided not to instigate formal supervisory proceedings under Article 27 FADP.

1.6 Insurance

SUPERVISION IN THE FIELD OF HEALTH INSURANCE

Clarification of roles and competences between FOPH and FDPIC

The FDPIC and the Federal Office of Public Health (FOPH) have taken steps to clarify their roles and increase their exchanges after the Swiss Federal Audit Office identified overlapping responsibilities in their supervision of health insurance companies.

Health insurance companies must comply with the provisions of social security law and data protection law when carrying out their activities. As a consequence, they are subject to the supervision of both the Federal Office of Public Health (FOPH) and the FDPIC. In the report dated 21 May 2021 on an audit carried out at the FOPH on supervision in the insurance sector, the Swiss Federal Audit Office (SFAO) found that there was need for clarification in relation to the roles of the FDPIC and of the FOPH, and that exchanges and coordination between the two authorities must be regulated (Audit EFK-20424).

Defining roles and rules for communication

In its assessment, the SFAO noted that the effectiveness of the FDPIC and FOPH's supervision of health insurance companies must be maintained or indeed increased. In supervising the health insurance companies, the FOPH's experience and familiarity with the subject through its on-site inspections must be exploited, as should the FDPIC's statutory powers, which have been strengthened by the total revision of the Federal Data Protection Act. The SFAO has therefore recommended that the FOPH should work with the FDPIC to define the roles and rules for the exchange of information between health insurance companies and the supervisory bodies in connection with non-compliant cases. The SFAO report also notes that the Federal Office of Justice (FOJ) has issued an expert opinion clarifying the responsibilities of the FDPIC and FOPH in implementing the data protection requirements, concluding that the responsibility is, in principle, that of the FDPIC. The FOPH has therefore decided to revise its Circular No 7.1 of 17 December 2015 on 'Data protection compliant organisation and processes for health insurance companies' accordingly.

Clarification of responsibilities

In his response to the SFAO's audit report, the FDPIC welcomed the coordination of the supervisory activities of the FOPH and the FDPIC in relation to health insurance, given their overlapping responsibilities, as well as the clarification of their roles and responsibilities. However, the FDPIC pointed out that the FDPIC's independence must remain unaffected by the efforts to coordinate health insurance matters and that he will continue to carry out his regulatory duties in relation to the FOPH.

Exchange has to be increased

In line with the SFAO's recommendation in its audit report, the FDPIC has been involved in the revision of FOPH Circular No 7.1. He made various proposals for amendments, in particular with regard to coordinating overlapping responsibilities. For example, the draft of the circular made it clear that the FOPH and the FDPIC should have regular exchanges in terms of their respective responsibilities, including discussions on an ad hoc basis if there is a need for coordination in an individual case or for effective supervision. It was also stated that the two supervisory authorities should cooperate with and support each other by exploiting their knowledge of their respective specialist areas of health insurance and data protection. In addition, insurers were advised that the removal of certain chapters in the new circular does not mean that insurers are no longer subject to the statutory requirements set out in these chapters. The circular specifies that the FDPIC acts as an independent supervisory authority and in accordance with his resources and priorities in relation to his responsibility for assessing conformity with data protection requirements as well as the substantive review of the processing regulations. The FOPH sent the new version of Circular No 7.1 to all health insurance companies in December 2021 and it came into force on 1 January 2022.

In the course of discussions on the revision of the circular, the FOPH and the FDPIC agreed to designate contact persons. In future, they will hold a meeting each year to discuss matters and will organise ad hoc meetings, as the SFAO recommended, to increase the effectiveness of their supervision.

1.7 Traffic and transport

POSTBUS AND SWISS FEDERAL RAILWAYS (SBB)

Security vulnerabilities on customer portals

During the year under review, PostBus's customer portal "ticketcontrol.ch" and SBB's platform "Nova" suffered data leaks as a result of inadequate security measures in their IT systems. The FDPIC checked that the companies' data protection officers had promptly taken the necessary action to remedy the vulnerabilities and inform their customers.

A group of journalists conducting an investigation were able to easily view and copy data from the customer portal "ticketcontrol.ch". They reported the data leak to PostBus, the company that operates the portal, and contacted us. The FDPIC immediately asked the company to comment. PostBus responded promptly, confirming the incident. The access logs were analysed, and the method of attack was verified relatively easily, and the attackers identified. During the course of further investigations, PostBus was able to prove to the FDPIC that the flaw on its customer portal had been rectified immediately after it was brought to its attention and that the exposed datasets had been deleted during the investigation.

Another flaw was reported to the FDPIC regarding the central public transport sales platform "Nova" operated by SBB on behalf of Alliance SwissPass, the Swiss national public transport organisation. An IT specialist investigator was able to retrieve a total of up to a million datasets including ticket and travelcard data within a short space of time. SBB confirmed the data leak to us and immediately fixed the flaw. It also informed the FDPIC that the other transport companies affected had also taken the necessary immediate action and that customers had not been adversely affected in any way. The IT specialist then deleted the data he had retrieved.

In both cases, the companies' data protection officers showed that, with the measures now in place, the platforms concerned no longer pose disproportionate systemic risks, and that the individuals concerned have been appropriately informed. Given the growing number of targeted attacks on IT systems, the FDPIC believes that all operators should devote more resources to keeping their systems secure. Furthermore, regular external audits should be carried out on systems that carry higher risks for the individuals concerned.

PASSENGER NAME RECORDS

Office consultation on the new act on the use of airline passenger data

The FDJP has worked on a legislative project for the use of airline passenger data (Passenger Name Records, PNR) collected by airlines to combat terrorism and crime in Switzerland. The FDPIC expressed his opinion during the office consultation.

When a passenger books a flight, they provide the airline or travel agency with a large amount of information. The security and police authorities are keen to use this information to combat terrorism and serious crime. Many European countries have already set up Passenger Information Units (PIUs) to collect, store and process airline passenger data. The data collected can, for example, be cross-checked against relevant law enforcement databases to identify individuals who may be involved in a terrorist offence or serious crime.

The Federal Council decided on 12 February 2020 that Switzerland should be allowed to use Passenger Name Records (PNR) as well. For that reason, in mid-2021 the FDJP and DETEC worked together to flesh out a bill to be submitted for consultation for a federal act on the collection and use of PNR data by Switzerland and disclosure of the same to countries whose data protection and data processing practices met the standards of the EU Directive 2016/681 of 27 April 2016 on the use of passenger name

record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (EU PNR Directive).

List of crimes needed

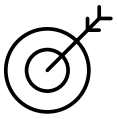
In his opinion on a first draft submitted, the FDPIC urges that the individual provisions respect the data protection principles. In particular, he demands that the scope of preventive action of PIUs be clearly defined and that the Federal Intelligence Service be granted only limited access to the PNR information system. Furthermore, an exhaustive list of crimes is needed indicating the purpose for which data may be collected. The FDPIC also points out that the principle of proportionality must be applied. For example, justification must be provided as to why a five-year retention period is necessary in order to achieve the intended purpose (see 28th Annual Report, Section 1.8).

PARKING APPS

Digital parking meters requiring entry of vehicle registration numbers

In the year under review, the FDPIC received a number of enquiries regarding digital parking meters requiring entry of vehicle registration numbers. He commented on these with reference to privately operated parking facilities. During the year under review, the large number of enquiries received from members of the public alerted the FDPIC to a growing number of digital parking meters. The FDPIC heard their concerns about whether registering by entering a vehicle registration number was acceptable from a data protection viewpoint.

Car parking facilities can collect and process licence plate numbers for registration purposes. However, the data may be stored only for as long as strictly necessary in order to achieve the intended purpose. In accordance with the obligation of transparency under data protection law, the data controller is required to inform the



data subject appropriately of the purpose of data collection and the associated data processing and data retention period if these are not already clear from the circumstances.

In particular, we informed enquirers that under Article 8 of the Federal Act on Data Protection they could request information from the controller of a data file as to whether, and if so which, data relating to them is being processed and for what purpose. Sample letters for requesting such information can be found on the FDPIC's website.

AUTOMATED DRIVING

Office consultation on the partial revision of the Road Traffic Act

The revision of the Road Traffic Act introduced a number of changes during the year under review such as provisions regulating automated driving in Switzerland. The FDPIC oversaw the project and expressed his opinion during the office consultation. He demanded that the explanatory notes on the Act clarify a few points regarding proportionality, with particular regard to the data retention period and data deletion. The Road Traffic Act (RTA) has been amended under the guidance of the Federal Roads Office (FEDRO) to allow automated driving in Switzerland. In future, the Federal Council will be able to determine the extent to which drivers may be relieved of their duties and the framework within which driverless vehicles equipped with automation systems may be permitted. Under the draft revision, such vehicles will be allowed to operate on specific routes under supervision.

Vehicles with an automation system must be equipped with a data storage system for automated driving (DSSAD) which cannot be deactivated and which records certain events related to the automation system such

as the time at which control of the vehicle is transferred from the driver to the system and vice versa. The DSSAD also records the times at which the system prompts the driver to take over control of the vehicle as well as any technical faults.

In the FDPIC's view, the information stored in the DSSAD can be easily linked to personal information, for example relating to the vehicle owner. Therefore, we welcomed the storage of time stamps without any location data. We also insisted that the RTA and its explanatory notes clearly set out who may access the data stored in the DSSAD and for which clearly defined purposes and whether or not – and, if so, when – such data may be analysed on an individual level. Among other things, this is to prevent data from being used for whatever purposes.

Furthermore, the FDPIC had questions regarding proportionality, for example in relation to the time limit for deletion of data, as data would be stored until the memory was full, meaning that storage time would vary depending on how much the vehicle was used. The FDPIC demanded that the explanatory notes cover this aspect in full detail and that they indicate the justification grounds for the deletion of data when vehicles are taken off the road.

The FEDRO has taken the FDPIC's suggestions on board in the draft. On 17 November 2021, the Federal Council adopted the dispatch to Parliament on the amendment of the Road Traffic Act.

NETWORKED MOBILITY DATA

Legal basis required to exchange mobility data

The federal government wants to promote efficient mobility, primarily by making it easier to combine different modes of transport. The key requirement for this is that the data and services required to make full use of the various mobility options are made available to users. The FDPIC has commented on the related bill in the course of the office consultation procedure.

The Federal Mobility Data Infrastructure Act (MODIG) creates the legal basis for the gradual development of a National Mobility Data Infrastructure (NaDIM), which enables the exchange of mobility data. The NaDIM is to be operated by a body known as the Mobility Data Agency (MDA). Private companies such as app developers and platform operators should thus be able to offer their customers mobility services that cover a range of transport networks.

Mobility data in terms of the bill is primarily factual data such as information about a transport system, timetables, fares, etc. A variety of personal information about customers is required for the reservation, booking and payment process, depending on what the offer entails. Under certain circumstances, data on a person's movements or – in connection with travel options for persons with reduced mobility – sensitive personal data may be generated and processed by the MDA. However, according to the FOT, the exact details are not yet known and will only become apparent as the project develops.

The FDPIC first requested that the required legal basis be created for the categories of data that the MDA processes. He also pointed out that the need for a data protection impact assessment in accordance with Article 22 of the new Data Protection Act must be considered in good time. This assessment will indicate the risks to personal privacy and informational self-determination inherent in the purpose, content, type, regularity or duration of the data processing required.

However, since according to the FOT the actual data processing and other important implementation details will only emerge as the project progresses, the FDPIC can only make a final statement on the entire project once the relevant information is available.


Reihe
Row
5

1.8 International

International cooperation in the past year was again dominated by the COVID-19 crisis. Practically all international conferences and meetings had to be held by video conference because of the pandemic. The 43rd International Conference of Data Protection and Privacy Commissioners, which was supposed to take place in Mexico in October 2021, was first going to be held in hybrid form, but eventually went ahead in virtual form only. After an initial postponement in 2021, the annual Conference of European Data Protection Authorities was cancelled altogether. The FDPIC also participated in various virtual events within the OECD this year, for example on the topics of "Data Governance and Privacy Challenges in the Fight against COVID-19" and "Data Localisation and Trusted Government Access to Data".

Where international meetings can only be held by video conference, this inevitably means that there are far fewer informal meetings and direct contacts. On the other hand, more data protection authorities and their officers can participate in video conferences than would otherwise be possible, because no travelling or related costs are involved.

The past year has illustrated the importance of the international dimension to data protection. Because many companies are active internationally, sensitive data protection issues arise, particularly in relation to the cross-border transfer of personal data, whether directly or through data storage in clouds and on servers abroad.

The FDPIC is therefore continuing to make its presence felt at an international level, participating actively in international bodies. These include the Council of Europe, the Conference of European Data Protection Authorities, the International Conference of Data Protection and Privacy Commissioners, the Francophone Association of Personal Data Protection Authorities and the OECD, as well as cooperation and coordination with the data protection authorities in the Schengen member states and exchanges with the European Data Protection Board (EDPB).

COUNCIL OF EUROPE

Protection of children's privacy in the digital world and guidelines regarding profiling as well as political campaigns

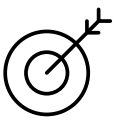
During its five meetings, the Consultative Committee on Convention 108 focussed, among other things, on fleshing out two documents adopted by the Committee of Ministers in 2021, namely the declaration on the need to protect children's privacy in the digital environment and the update of the Committee of Ministers' recommendation on profiling. The Committee also adopted guidelines on the protection of individuals with regard to the processing of personal data by and for political campaigns.

As in the previous financial year, the meetings of the Consultative Committee of the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) were held online in 2021 due to the pandemic. The meetings of the office in which an FDPIC representative serves also had to be held online. The Committee dealt with data protection issues in a number of key areas. It also adopted its Work Programme 2022–2025. Among other things, the Committee expressed its opinion on the draft second additional protocol to the CoE Convention on Cybercrime

(Budapest Convention). In particular, it stressed the importance of introducing a data protection regime that guaranteed effective law enforcement while at the same time protecting data subjects.

The Committee was involved in preparing two documents adopted by the Committee of Ministers in 2021. The first was the Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment. This document was fleshed out by the CoE Steering Committee for the Rights of the Child in co-operation with the Consultative Committee and urges Member States to step up efforts to protect children's privacy and personal data, especially health-related data and data collected in educational settings. This was particularly important in the context of the COVID-19 pandemic in order to minimise potential adverse effects of public identification of a child as a COVID-19 carrier.

The second document was the Recommendation on the protection of individuals with regard to the processing of personal data in the context of profiling. The Recommendation provides that respect for fundamental rights and freedoms should be guaranteed in all profiling operations in both the public and private sectors. This document is an update of a previous declaration adopted in 2010 and takes into account the technological advances of recent years, aligning its text with the modernised data protection Convention 108, known as "Convention 108+".



In its statement "COVID-19 vaccination, attestations and data protection", the Committee stressed the importance of striking a balance between protecting fundamental rights and freedoms and the risks to public health arising from the pandemic.

The Committee also adopted guidelines on the protection of individuals with regard to the processing of personal data by and for political campaigns. These guidelines regulate the application of the modernised data protection convention, "Convention 108+", to political campaigns, recognising the increasing use of digital campaigning strategies via social media.

The Committee also decided to update the standard Council of Europe treaty on the appropriate level of protection in the context of transborder data flows. The work, for which Switzerland is the rapporteur, is still at an early stage.

EUROPEAN CASE HANDLING WORKSHOP

Strengthening cooperation among data protection authorities

As per tradition, the FDPIC attended the European Case Handling Workshop again, this time hosted by the Gibraltar Regulatory Authority.

Due to the pandemic, the event was held online on 16–17 November 2021. It was attended by more than 120 participants from 30 data protection authorities, who discussed matters relating to data breach notifications, internal handling of complaints, enforcement action and the implications of the European Court of Justice judgment commonly referred to as 'Schrems II'. The aim of the event was to strengthen cooperation among data protection authorities and, in particular, to make it more efficient.

The case handling workshop is invaluable, especially to smaller regulators, as it provides a platform through which authorities can share their experiences and expertise. In view of the entry into force of the new Federal Act on Data Protection (see Focus I) and the administrative assistance provided for in it, this sharing and development of expertise will become important for the FDPIC. Therefore, the FDPIC has also offered to host the European Case Handling Workshop in Switzerland in autumn 2023.

GLOBAL PRIVACY ASSEMBLY

Online meeting of more than 90 members and observers

The 43rd Global Privacy Assembly (GPA), formerly known as the International Conference of Data Protection and Privacy Commissioners, took place on 18 – 21 October 2021 and was held online for the second year in a row because of the pandemic.

The online conference was hosted by the National Institute for Transparency, Access to Information and Personal Data Protection (INAI) in Mexico and was attended by more than 90 members and observers to consider key data protection challenges. Its theme was "Privacy and Data Protection: A Human-Centric Approach".

A fundamental right

The 43rd Closed Session of the Global Privacy Assembly (GPA) was opened by UK Information Commissioner Elizabeth Denham, who praised the work of the privacy community during the pandemic, calling for the Assembly to continue to be impactful.

"With this Conference, we aim to shift the thinking from the protection of personal data to the protection of the privacy as a fundamental right," said conference host Blanca Lilia Ibarra Cadena, president commissioner of Mexico's National Institute for Transparency, Access to Information and Personal Data Protection.

Resolutions were discussed in the closed session and approved during the meeting, giving a shared view on a range of important current topics:

- Data sharing for the public good;
- Children's digital rights;
- Government access to data;
- The future of the Global Privacy Assembly;
- International enforcement cooperation; and
- Regulatory sandboxes.

New strategic plan

Conference participants adopted a new two-year strategic plan for the GPA that seeks to create an environment in which privacy and data protection authorities can practically fulfil their mandates to ensure high standards of data protection globally and promote and facilitate effective regulatory cooperation.

The GPA also announced the recipients of the 2021 Global Privacy and Data Protection Awards, which celebrate the achievements of global privacy officers and highlight notable investigations, good practices and public outreach initiatives.

GLOBAL PRIVACY ASSEMBLY

Privacy protection in international development aid

Established a year ago, the Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management (WG AID) reports on its activities.

The Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management (WG AID) was established by a resolution of the Global Privacy Assembly (GPA) at its 42nd annual meeting in 2021. Chaired by the FDPIC, the WG AID has more than 20 members, and its composition reflects the geographical diversity of the GPA.

In its first year of existence, WG AID has focused its energy on developing a work plan in line with the GPA's strategic priorities, including the following in particular:

- the advancement of privacy protection worldwide
- the strengthening of relations with other international bodies and networks that advance data protection and privacy issues, including through agreements with observer bodies
- human rights, social protection and democratic rights

General goals

In accordance with the priorities set out in the resolution, the members of the WG AID have set themselves the following general goals:

- to respond to requests for cooperation from relevant parties (e.g. development agencies or humanitarian actors) to develop guidelines and share best practices in privacy and data protection, taking into account the specific characteristics of international development aid and international humanitarian action as well as the need to facilitate these activities
- to develop an advocacy and engagement strategy with relevant stakeholders

In order to achieve these two goals, the WG AID has decided to implement the following activities:

- Refine its understanding of international development aid, international humanitarian aid and crisis management
- Establish sustained contacts with the relevant actors, at both bilateral and multilateral levels and thus maximise the reach of the GPA's voice by strengthening relations with international development aid actors
- In collaboration with other relevant working groups of the GPA, produce documents and advocacy tools for better consideration of data protection and privacy in relevant activities
- Promote and facilitate, for the recipient countries benefiting from these activities that do not have legislation on data protection and privacy, their integration into the global data protection and privacy community

As part of their activities, the members of the WG AID have mapped international development aid and international humanitarian aid. They have also identified recipient countries benefiting from these activities that do not have legislation on data protection and privacy. Furthermore, the WG AID has created a questionnaire and a cover letter that will enable it to refine its understanding of the work of the relevant actors.

SCHENGEN INFORMATION SYSTEMS

SIS II, VIS and Eurodac Supervision Coordination Groups

The SIS and VIS Supervision Coordination Groups (SCG) approved a joint letter on the legislative proposal of the EU Commission to amend the Schengen evaluation mechanism.

The two meetings of the three Supervision Coordination Groups on the EU's SIS II, VIS (chaired by the FDPIC) and Eurodac information systems had to be held by video conference again this year due to Covid restrictions. The meetings took place on 16 – 17 June 2021 and 24 – 25 November 2021 and were attended by the European Data Protection Supervisor (EDPS) and the national data protection authorities of the Member States.

The VIS Supervision Coordination Group adopted a questionnaire on advance deletion of data. Advance deletion of data is required when an individual has acquired the nationality of a Member State and therefore no longer requires a Schengen visa. The data protection authorities of the Member States have been urged to have the questionnaire completed at national level in order to check to ensure that advance deletion is being carried out in the various States.

At the meeting in November, the SIS and VIS Supervision Coordination Groups drafted and approved a joint letter on the EU Commission's legislative proposal to amend the Schengen evaluation mechanism. In particular, the letter stressed the importance of involving experts from the data protection authorities in the Schengen evaluations focussing on data protection. It was also noted that the experts should be called in earlier than planned, namely four months in advance instead of just eleven weeks. The letter was sent to the European Parliament, Council and Commission.

The Eurodac SCG and the European Union Agency for Fundamental Rights (FRA) adopted a guide on the right to information for authorities when taking fingerprints for Eurodac. The guide was distributed to the competent authorities in Switzerland and was published on various websites.

UNITED KINGDOM

Adequate level of data protection post-Brexit

There are no changes to the UK's adequacy status from Switzerland's perspective. The UK is still on the FDPIC's list of countries that offer an equivalent level of data protection.

VIDEO CONFERENCE SYSTEMS

Best practice recommendations from data protection authorities

Since the beginning of the pandemic, authorities and private companies have increasingly been making use of video communication platforms. The FDPIC, in cooperation with five data protection authorities from other countries, gave the video teleconferencing companies Microsoft, Google, Cisco and Zoom the opportunity to present their teleconferencing platforms and enter into an open dialogue with the authorities.

In the exchange with the video teleconferencing companies, the authorities focused on topics such as 'security', 'privacy by design and default', 'know your audience' and 'transparency'. The dialogue proved beneficial for all sides. The dialogue resulted in a statement with possible best practices, which is available on the FDPIC website. A number of those measures are listed here (see Box on next page).

It is also important that providers of videoconferencing services build trust with their users by processing information about them only as they may expect from the circumstances. Personal data should only be collected to the extent that it is necessary for the use of the core functions of the videoconferencing service. It should be made completely transparent to users where the data is stored and through which channels it is transported. Users should also be given the choice of which locations their personal data is forwarded through and where it is stored.

The document published on the website is not exhaustive, and companies providing corresponding services must also observe the data protection provisions applicable in Switzerland and the FDPIC's comments on the transfer of data abroad.

Security

- Regular testing of security measures is vital to ensure they remain robust against constantly evolving threats
- Regular staff training on data protection and security
- Regular audits of third parties, including logging sub-processor access to personal information and a principle of least privilege approach to access controls

Transparency

- Users should be informed about how and why their data is collected and used
- Users should be clearly informed about who their data is being given to and why

Approaches to privacy by design und default

- Privacy impact assessments should be completed before implementing new video teleconferencing solutions and functions, and regular contact should be established between privacy, security and development teams
- Adhere to the data minimisation principle
- Video teleconferencing companies should by default adopt the highest privacy settings for their service

Know your audience

- Video teleconferencing companies must put in place robust data protection and security measures to appropriately protect personal data in sensitive contexts such as education and healthcare
- Tailored privacy and security guidance for specific groups is necessary to ensure that the security requirements of using a video teleconferencing service are met for all users and that they can choose the settings and features that are most appropriate for them

End-to-End encryption

- End-to-end encryption should be available where the meeting host creates the key and that only they and meeting participants have access to it
- The use of end-to-end encryption by default in sensitive one-on-one settings, such as tele-health is important

Personal data transfers with reference to foreign countries

STANDARD CONTRACTUAL CLAUSES (SCC)

The transfer of personal data to a country with an inadequate level of data protection

In his opinion of 27 August 2021, the FDPIC confirms that he recognises the EU Standard Contractual Clauses as the basis for personal data transfers to countries lacking an adequate level of data protection. He states that adjustments and additions are needed for the clauses to be used under Swiss data protection law.

The Swiss Federal Act on Data Protection (FADP) states that personal data may not be disclosed to countries lacking an adequate level of data protection. Exceptions are made in cases in which an adequate level of protection can be guaranteed in the receiving country, for instance by means of a contract. Whether or not contractual agreements are an effective means of ensuring adequate protection of the personal data to be transferred must be verified in each individual case. The FDPIC has published a guide to checking the admissibility of data transfers to foreign countries on his website.

If data protection can be guaranteed by means of a contract, then the Standard Contractual Clauses (SCC) adopted by the European Commission with its implementing decision (EU) 2021/914 of 4 June 2021 are an effective tool for data transfer.

In his opinion of 27 August 2021, the FDPIC confirms that he recognises these new SCCs, which refer to the EU General Data Protection Regulation (GDPR), including all modules, provided that they are adapted and/or supplemented as necessary in each individual case. The FDPIC explains that firstly one needs to select the relevant scenario (data exporters and data importers can be data processors as well as data processing contractors) and then one needs to determine the law governing the data transfer (Swiss data protection law only or both Swiss and European data protection law). The clauses will then need to be modified accordingly, with particular regard to the competent supervisory authority, the applicable law for contractual claims and the place of jurisdiction. Further details can be found in the FDPIC's opinion available on his website.

Under current law, the FDPIC is to be notified of any use of the recognised SCCs in advance of any data transfer. Under the revised FADP, this requirement will no longer apply.

DATA TRANSFERS TO FOREIGN COUNTRIES

Guide to checking the admissibility of data transfers in accordance with Article 6 para. 2 let. a FADP

As a follow-up to the position paper of 8 September 2020 on the Privacy Shield Regime, the FDPIC has published a guide to checking the admissibility of data transfers to foreign countries in accordance with Article 6 para. 2 let. a FADP. In the absence of sufficient contractual guarantees or additional safeguards, data transfer abroad is unlawful.

The guide published on the FDPIC's website is intended to help data controllers check the admissibility of data transfers to foreign countries. It uses a flow chart and a questionnaire to explain the case of data transfer to a country that lacks legislation guaranteeing adequate protection, in which case sufficient alternative safeguards are required in order to eliminate or compensate for the deficiency (Art. 6 para. 2 let. a FADP).

If a country is not on the FDPIC's list of countries with an adequate level of data protection or if there are insufficient safeguards in place to ensure that transferred data is protected, after assessing the specific case at hand, the exporter must take additional measures such as contractual arrangements with the importer. These typically take the form of Standard Contractual Clauses (SCC) (see article on the left).

When applying SCC, it must be examined whether these are not sufficient in themselves, for example, because inadequate rules of the law applicable to the contracting party take precedence over such clauses. In such cases, it needs to be verified whether or not the four fundamental safeguards (principle of legality, principle of proportionality, availability of legal remedies and the guarantee of legal recourse) are guaranteed in the applicable foreign law. As an aid, the FDPIC has included a questionnaire in the guide, tailored to US law and based on similar questionnaires of the NGO noyb (My Privacy Is None Of Your Business), founded by Maximilian Schrems.

If the laws to which the contracting party is subject provide all the necessary guarantees, then the SCCs are sufficient, unless further contractual safeguards are required. These may include, for example, provisions affording enhanced rights to data subjects (e. g. right to information) or specific technical measures as a condition for data transfer.

However, if the laws to which the contractual partner is subject do not provide all of these guarantees, then the exporter needs to consider additional contractual measures as well as organisational measures and/or, in particular, technical measures. If such measures cannot compensate for the lack of protection identified, the data transfer abroad is unlawful and must be suspended or terminated immediately.

Risks and requirements associated with the authorities' use of public clouds

During the year under review, the FDPIC continued to focus closely on the topic of cloud computing. During office consultations and in his advisory meetings with a working group of the Federal Administration, he pointed out the risks and requirements associated with the outsourcing of personal data processing by public authorities to public cloud providers.

In connection with the Andrey interpellation of 16 September 2021 regarding the awarding of public cloud services to US and Chinese companies, the FDPIC pointed out to the Digital Transformation and ICT Steering Sector (DTI) of the Federal Chancellery that even if cloud services were to be sourced from trusted European providers, they may still be subject to the applicability of sometimes problematic foreign laws and the risk of disproportionate access by the authorities of the countries concerned. He also explained that a cloud provider had to be able to maintain professional secrecy as well as ensuring data security. Finally, the FDPIC stressed that regardless of the destination country, the outsourcing of personal data to third parties inevitably increased the risks to data integrity, availability and confidentiality, and therefore a risk impact assessment had to be carried out.

The FDPIC also commented on the Marti Interpellation of 30 September 2021 regarding Microsoft cloud services: He pointed out to the DTI that, with respect to the ongoing work of the Federal Administration, major decisions regarding the use of cloud services offered by Microsoft or other providers could only be made after an analysis of the legal basis, the creation of an information security and data protection concept, and a risk analysis including data protection risks. We stressed the need to examine alternative offerings given that the cloud could also be used to store text content as well as telemetry and user data. In this context, we reiterated the data protection requirements, which establish an obligation to implement technical measures to effectively prevent disproportionate access to data by the authorities of the destination country.

The FDPIC also attended, in an advisory capacity, the meetings of an ad hoc working group led by the Legal Affairs Section of the Federal Chancellery on the report on the legal framework for cloud services. The report is part of the Federal Administration's cloud strategy and aims to clarify the legal situation regarding the use of public clouds by the Federal Administration. Clarification of the legal situation is all the more urgent given the pace at which the Federal Administration's projects based on cloud computing solutions are currently taking shape.

The FDPIC and other data protection authorities across Europe are currently in the process of developing a policy for the outsourcing of personal data processing by public authorities to US public cloud service providers in particular. Although neither EU law nor the CJEU's rulings are applicable in Switzerland, the FDPIC takes into account European regulatory developments in formulating his policy, striving for an EU-equivalent level of data protection when applying federal data protection legislation in light of the mutual adequacy decisions of the EU and Switzerland. In this context, it is also remarkable that the president of the European Commission and the US president jointly announced their intention at the end of March 2022 shortly to replace the Privacy Shield framework – which was invalidated by the CJEU (see 28th Annual Report, Focus II) – with an enhanced data privacy framework.

SCHREMS II

European Data Protection Board (EDPB), Borders, Travel & Law Enforcement Subgroup (BTLE ESG)

The FDPIC took the opportunity to discuss Schengen-related matters with the European Data Protection Board (EDPB) and to exchange views with the other European authorities. During the year under review, the focus was on the impact of the Schrems II judgment and the data protection authorities' response to it.

The FDPIC participated actively in the Borders, Travel & Law Enforcement Subgroup (BTLE ESG) mainly in the first half of the reporting period. The working group focused closely on the Schrems II issue and developed the recommendations for the EDPB. During its June 2021 plenary session, the EDPB adopted a final version of the recommendations on supplementary measures following public consultation. The recommendations aim to assist controllers and processors acting as data exporters with their duty to identify and implement appropriate supplementary measures where they are needed to ensure an essentially equivalent level of protection to the personal data they transfer to third countries.

On 18 June 2021, the FDPIC published a guide to checking the admissibility of data transfers to foreign countries based on Swiss law (see article above: Guide to checking the admissibility of data transfers in accordance with Article 6 paragraph 2 letter a FADP).

Freedom of Information

2.1 General

The Freedom of Information Act seeks to promote transparency with regard to the mandate, organisation and activities of the Administration. To this end, it contributes to informing the public by ensuring access to official documents (see Art. 1 FoIA). In applying the principle of freedom of information, the Administration aims to increase confidence in the State and the authorities by creating a greater understanding and, consequently, acceptance of their actions.

The figures provided by the Federal Administration regarding the number of requests received in 2021 for access to official documents indicate that the media and society's need for specific, transparent information is as strong as ever. In the year under review, the federal authorities again received more requests for information than in the previous year. In the second year of the pandemic, almost one in four of the sometimes extensive and complex requests again concerned official documents relating to COVID-19.

Many of the information requests required extensive resources to process, not least because they often necessitated coordination with other offices and departments. Overall, implementing freedom of information again proved to be a demanding and challenging task during a pandemic. The figures in Section 2.2 show a continuation this past reporting year of the trends observed in recent years, namely a steady increase in information requests and a constantly high proportion of cases in which access was granted in full.

If the applicants or third parties affected by the granting of access do not agree with the authorities' granting access, the Freedom of Information Act entitles them to submit a request for mediation to the FDPIC. Here, too, there is a clear trend: The FDPIC received 149 mediation requests during the year under review, an increase of 60% on the previous year.

The purpose of mediation is to reach a swift agreement between the parties. The measures introduced for this purpose with the pilot project in 2017, and, in particular, the primacy of the oral mediation procedure, proved successful again in 2021. An analysis of the mediation requests processed in 2021 shows that where a mediation session was held, an amicable solution was reached in 67% of cases. By contrast, in the 40 mediation procedures in which a mediation session could not be held because of the pandemic, an agreement was reached in only 5% of cases. When the Federal Council introduced the requirement to work from home on 13 January 2021 in view of the tense epidemiological situation and limited gatherings in public spaces to no more than five people, among other measures, this also had a direct impact on the way in which mediation procedures were conducted. As a result, the FDPIC was forced to suspend face-to-face mediation sessions with the parties between January and June 2021. Therefore, many mediation procedures had to be conducted by correspondence instead. This led to a lower proportion of amicable outcomes and longer processing time for mediation procedures in the year under review, resulting in a backlog in the completion of procedures (see Section 2.3).

Accordingly, the figures clearly show that face-to-face mediation sessions held in-situ help conclude mediation proceedings in little time. However, the growing number of mediation requests over the years and the increasing complexity of the requests also means that the FDPIC is exceeding the statutory processing time of 30 days in an increasing number of cases. The FDPIC believes that, without additional resources, this negative trend is likely to be exacerbated, making swift processing, as required by law, increasingly difficult to achieve (see Section 2.3 for more details).

COVID-19 vaccine procurement contracts

The FDPIC's recommendation of 18 January 2022 following a mediation request received in the year under review, attracted a great deal of public attention. The FDPIC recommended that the FOPH grant access to the COVID-19 vaccine procurement contracts after consulting the pharmaceutical companies concerned and taking into account the principle of proportionality. In his substantiated recommendation, the FDPIC pointed out that he had to take into account the changed circumstances when reassessing the exceptions justifying a deferral of access. Among other things, the FOPH itself had stated that vaccines were no longer in short supply, therefore the FDPIC saw no sufficient reason to further defer the processing of the information requests received, also in view of the fact that the required consultations with the pharmaceutical companies would take time. The FDPIC's recommendation is in line with the Parliament's decision not to enshrine in a special law the obligation to disclose the vaccine contracts in question as put forward by the National Council. As this special provision has not been adopted, the Freedom of Information Act applies, as is clear from the Council of States' debates. Under the Act, the FDPIC recommended that the FOPH grant the access that had been deferred.

2.2 Access requests – Further increase in 2021

According to the figures provided by the federal authorities, 1385 access requests were submitted to them in the year under review, compared with 1193 in 2020, equating to an increase of 16%. The authorities granted full access in 694 cases (50%), compared with 610 (51%) in 2020. In 324 cases (23%), access to the documents requested was partially granted or deferred, compared with 293 (25%) the year before. Access was completely denied in 126 cases (9%), compared with 108 (9%) in 2020. According to the authorities, 48 requests for access were withdrawn (compared with 35, or 3%, in 2020), 78 requests were still pending at the end of 2021, and in 115 cases there was no official document.

Growing public awareness of the principle of freedom of information due to media coverage is a contributing factor as more people take up the opportunities this principle presents. This trend is expected to continue in the coming years.

Another reason for the increase in access requests is the need for information and transparency in relation to the measures introduced during the COVID-19 pandemic. The authorities produced statistics on requests for access to documents relating to COVID-19, which it sent to the FDPIC along with the information to be reported annually (see Statistics on Requests for access 2021 with Corona reference). According to the authorities, 336 out of 1385 access requests (24%) were for documents relating to COVID-19. Full access was granted in 121 cases (36%), i. e. less frequently compared with the overall statistics. The authorities granted partial access or deferred access in 131 cases (39%), therefore more frequently in relation to COVID-19 documents, while access was denied completely in 13 cases (4% or half the overall percentage). Eighteen requests for access were withdrawn, 29 requests were still pending at the end of 2021, and in 24 cases there was no official document. Society is likely to continue to evaluate the government measures introduced to combat the pandemic until well after the health crisis is over, meaning that further access requests and mediation requests relating to the pandemic can be expected in 2022.

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

Federal departments and federal offices

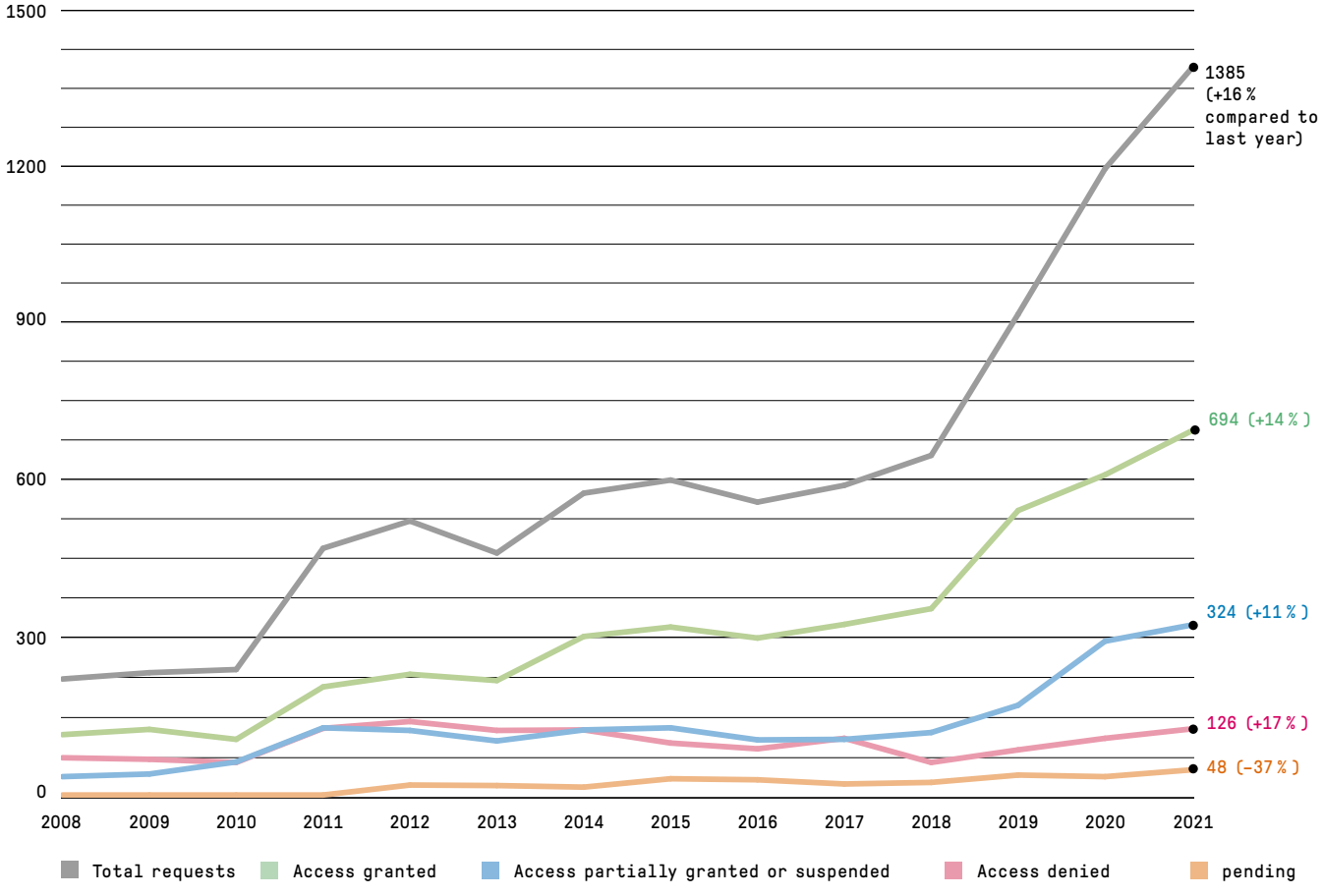
Various administrative units were again the focus of much media and public attention in 2021, year two of the COVID-19 pandemic. Due to the nature of their work, the FDHA and the DDPS, in particular, received a large number of access requests. In the case of the FDHA, 63% of the requests received by all offices were for access to official documents relating to COVID-19. The authorities in question reported that the requests received were sometimes complex and extensive, with many of them required time-consuming coordination between federal offices and departments. The authorities in question reported a heavier workload than before the pandemic, with the situation expected to continue in 2022.

The figures released by the federal offices indicate that the FOPH received the most requests for access in the year under review, namely 251 – 217 of which for access to Covid-related documents – followed by the FOSPO with 172, swissmedic with 72 and the FOEN with 64. The departments which received the most requests are the FDHA (422), the DDPS (281) and the FDFA (156). Thirteen authorities reported receiving no requests for access during the year under review. The FDPIC himself received 16 access

requests and granted full access in seven cases; he granted partial access or deferred access in two cases and denied access altogether in two further cases. Five requests were still pending at the end of 2021.

In 2021, fees charged for obtaining access to official documents totalled CHF 14,924.90, only slightly lower than last year (CHF 15,189.30). While the FDFA, the DETEC, the Parliamentary Services and the Office of the vAttorney General of Switzerland did not charge any fees, the other five departments and the Federal Chancellery did invoice applicants for some of the time spent dealing with their requests (FDHA: CHF 7665.20; EAER: CHF 4052.70; FCh: CHF 1150; DDPS: CHF 950; FDF: CHF 750; FDJP: CHF 357). It should be noted that just 19 out of 1385 requests for access incurred a fee. Compared with the previous year, when fees were charged in 25 cases, both the number of cases in which a fee was charged and the total amount charged were lower. This is remarkable considering that the number of requests for access was much higher. Therefore, as in previous years, fee-charging remains the exception, with access being granted free of charge in more than 98% of cases. Implemented again in the year under review, the administrative practice of granting free access to official documents is to be enshrined in law. On 1 December 2021, the Council of States joined the National Council in considering a parliamentary initiative to this effect. According to the initiative, in future, the authorities should only charge fees for requests that take

Figure 1: Evaluation of requests for access – trend since 2008



particularly long to process. Parliament will now decide on the terms and implementation of the principle of free access to official documents and any exceptions.

As regards working hours spent processing access requests, the FDPIC reiterates that the authorities are under no obligation to record these hours and that there are no legal requirements establishing a standard recording procedure applicable to the entire Federal Administration. Data is sent to the FDPIC on a purely voluntary basis and therefore reflects only a portion of the time actually spent handling requests. According to the data received, the time spent this reporting year was 5,562.35 hours, up from 2020 (5,010 hours).

The fact that the time spent processing information requests notified by the authorities only partially reflects the actual time spent is illustrated by the data reported by the FOPH for

instance. In addition to the 208.5 working hours notified by the FOPH's competent specialist units and the legal support provided by its adviser, amounting to 40% full-time equivalents, the FOPH reported setting up its own implementation structure and specific processes for dealing with the large number of access requests in connection with COVID-19. According to the FOPH, the amount of work involved in the year under review was very high, amounting to at least 3.9 FTEs. The same applies to other units of the Federal Administration.

The time devoted to preparing mediation procedures also increased, totalling 864.6 hours (compared with 569 hours in 2020, 473 hours in 2019, 672 hours in 2018 and 914 hours in 2017).

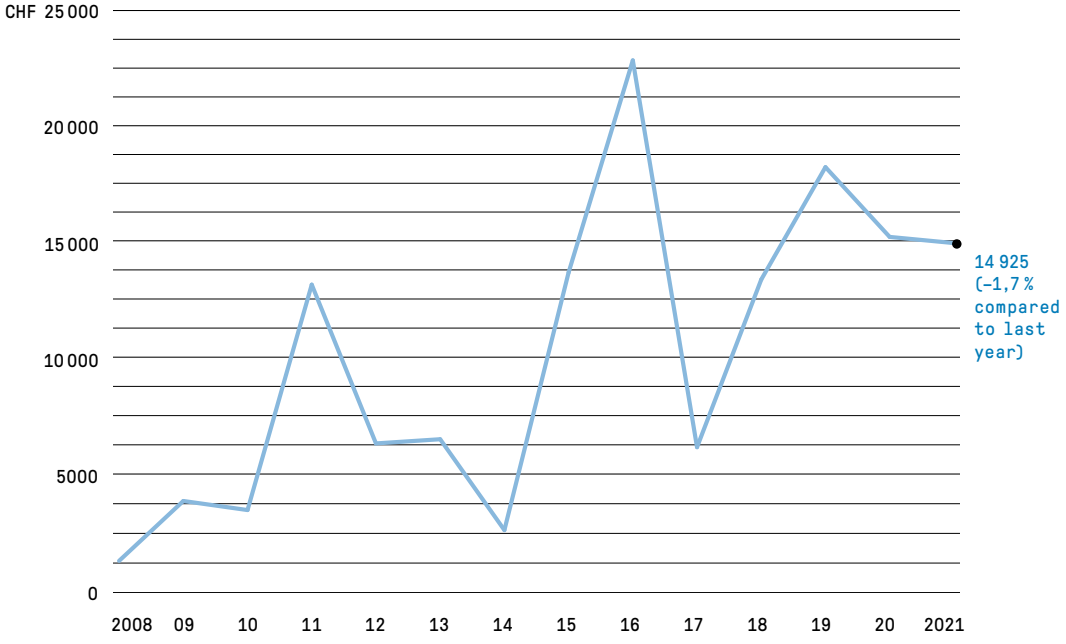
Parliamentary services

The Parliamentary Services informed us that they had received one request for access, which they upheld, granting full access to the requested documents.

Office of the Attorney General of Switzerland

The Office of the Attorney General of Switzerland announced that it had received eight access requests in 2021. Access was denied outright in four cases, and in one case the request was withdrawn. As for the three remaining cases, there were no official documents.

Figure 2: Fees charged since the FoIA entered into force



2.3 Mediation procedure – significant increase in mediation requests

In 2021, the FDPIC received 149 mediation requests, 60% more than in 2020 (93 requests). The majority of mediation requests was submitted by the media (53) and private individuals (49). Therefore, of the 565 cases in which the Federal Administration fully or partially denied access, deferred access or stated that there were no official documents, 149 cases (26% of all unmet requests for access) resulted in a mediation request being submitted to the FDPIC. Thirty-one of these (21%) concerned official Covid-related documents.

In 2021, 139 mediation requests were settled, of which 126 had been submitted during that year and 40 the previous year. In 50 cases, the participants were able to reach a mutually acceptable agreement. The FDPIC also issued 49 recommendations, enabling him to settle 65 cases which were unlikely to result in an agreement between the parties.

The cases dealt with include seven mediation requests which were not submitted on time, 17 cases which did not satisfy the conditions for application of the Freedom of Information Act, and two requests that were withdrawn.

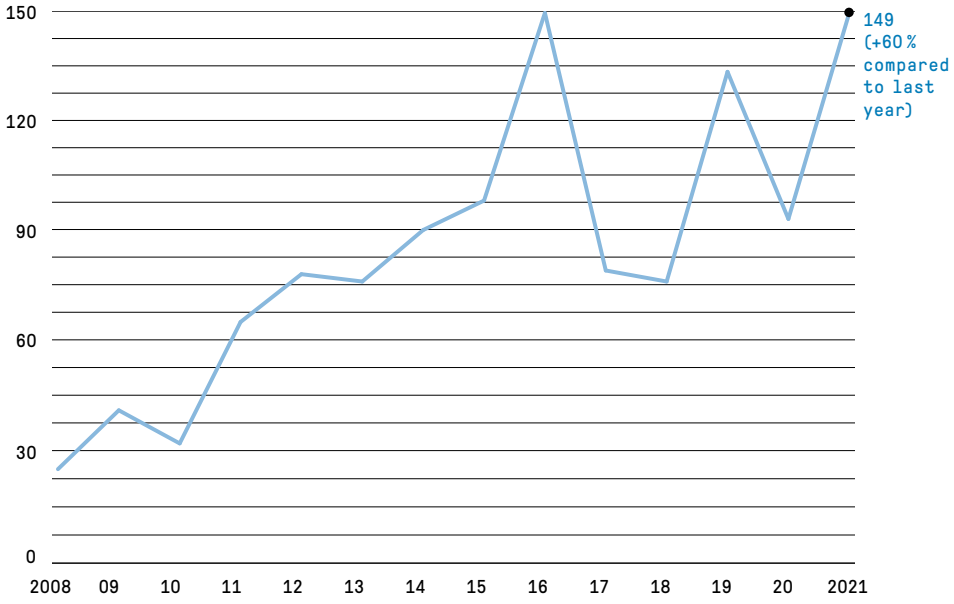
At the end of the year, eight mediation procedures had been suspended by agreement between the participants or at their request.

Proportion of amicable outcomes

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

The ratio of amicable outcomes to recommendations is the best measure of the effectiveness of the measures introduced in 2017 and of oral mediation sessions. During the year under review, 50 amicable outcomes were achieved, and the FDPIC issued 49 recommendations to settle 63 cases. There-

Figure 3: Mediation requests since the FoIA entered into force



fore, the ratio of amicable outcomes to recommendations is 44%. However, this needs to be explained: amicable solutions are typically only reached when mediation sessions take place. In the 45 mediation sessions that took place during the year under review, an agreement was reached in 30 cases (67%). As mentioned in Section 2.1, face-to-face mediation sessions with the parties had to be suspended between January and June 2021 because of the measures introduced to stop the spread of COVID-19, and so 40 sessions had to be cancelled. The impact on the proportion of amicable outcomes was inevitable: agreement was only reached in two (5%) of the procedures conducted by correspondence.

Therefore, we can conclude that oral mediation sessions continue to be effective in reaching amicable solutions. In the FDPIC's view, oral mediation should continue to be favoured over mediation by correspondence and should be promoted accordingly. Oral mediation sessions prove beneficial for all parties involved in the mediation procedure. In some cases, because of the Covid measures in place, the parties requested that the procedure be suspended until oral mediation sessions could be resumed.

All the recommendations issued in the year under review are available on the FDPIC's website.

Table 1: Amicable outcomes

2021 (Corona)	**44%**
2020 (Corona)	34%
2019	61%
2018	55%

Duration of mediation procedures

The table 2 on the following page is divided into three sections according to processing time. It should be noted that the processing time indicated does not include the period during which a mediation procedure is suspended at the participants' request or with their consent. A mediation procedure is typically suspended when an authority wishes to re-examine its position after the mediation session or has to consult the third parties involved. If a mediation session is postponed at the request of one of the parties (due to holidays, illness etc.), the processing time does not include the period of time between the originally scheduled date and the rescheduled date or the period of time by which the proceedings are extended.

The table 2 shows that 42% of mediation procedures completed in 2021 were concluded within the 30-day period, while 51% took between 31 and 99 days, and 7% took 100 days or more.

In most cases, the statutory 30-day deadline for completing the mediation procedure can be met, provided the mediation sessions are held according to schedule – i. e. without the parties requesting any postponements – and culminate in agreement within the time limit from receipt of the request. In the year under review, the 30-day deadline was met in 60% of cases in which an agreement was reached.

The large number of mediation requests submitted to the FDPIC in 2021 meant that in some cases it was

already clear the moment a request was received that the 30-day deadline would not be met. Given the limited human resources available for processing the mediation requests, the deadline had already expired by the time the mediation sessions were due to take place.

Furthermore, of the 59 mediation requests settled within the 30-day period, only 31 (53%) mediation procedures were settled by agreement or with a recommendation following a discussion of the issues that were the subject of mediation. In the other 28 cases (47%), no substantive assessment was made. These were mainly cases that fell outside the scope of the Freedom of Information Act or in which the formal requirements for initiating mediation were not met.

As mentioned earlier, in-situ mediation sessions had to be suspended between January and June 2021 because of the COVID-19 pandemic. As a result, very few amicable outcomes were achieved in the mediation procedures that fell within that time frame (in just 5% of cases). Where no agreement is reached, the FDPIC has to issue a written recommendation. Conducting mediation procedures in writing and issuing recommendations typically increase the FDPIC's workload significantly, resulting in longer processing time for the individual procedures and affecting the following procedures and the time needed to complete them. In that sense, the rules introduced due to the COVID-19 pandemic were among the factors that contributed to increasing the duration of mediation procedures, resulting in a processing backlog. When there is already a backlog in the processing of mediation procedures, each new request received only compounds this. In the year under review, the FDPIC was able to issue written recommendations to the parties involved within the statutory period of 30 days of receipt of the request only in four cases (7%).

Failure to meet the deadline was also often due to unavailability of the people or authorities concerned (due to holidays, illness or travel), the large number of third parties involved in the procedure, or the need to resolve complex legal issues. These explanations also apply to the nine cases that took 100 days or more to process. Consultations conducted abroad, multiple negotiation rounds among the participants, and the involvement of a large number of documents or people were other factors that made it hard to meet

Table 2: Processing time of mediation procedures

Processing time in days	2014-August 2016*	Pilot phase 2017	2018	2019	2020	2021
within 30 days	11%	59%	50%	57%	43%	42%
between 31 and 99 days	45%	37%	50%	38%	30%	51%
100 days or more	44%	04%	00%	05%	27%	7%

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

deadlines. The above-mentioned situations frequently entail a substantially higher workload, and in such cases – in accordance with Article 12a of the Freedom of Information Ordinance (FoIO; RS 152.31) – the FDPIC may extend the deadline by an appropriate period.

The legislator has designed the mediation process as an informal and non-prejudicial forum for amicable resolution of disputes. However, experience shows that the involvement of legal representatives by the applicants or by third parties being interviewed at the access and mediation procedure stage is not conducive to a straightforward, pragmatic and swift solution.

While exceeding the tight deadline of 30 days in complex cases and in procedures involving several parties (i. e. several third parties affected) is regarded as inherent in the system given the possibility of extension provided for by law, the renewed increase in the number of deadlines exceeded – which can only be explained by insufficient human resources – constitutes undue delay from a legal standpoint.

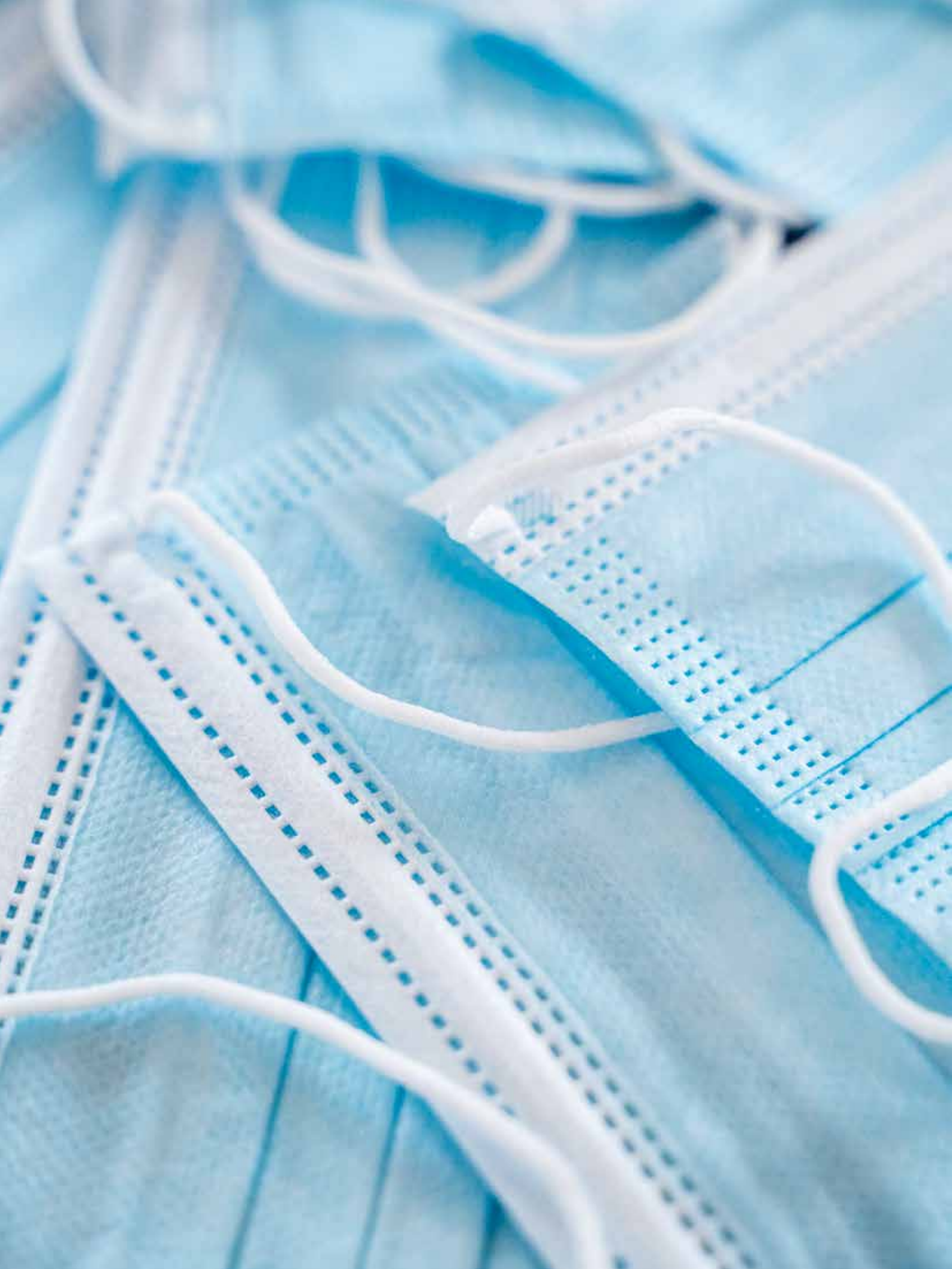
Number of pending cases

The figures below (see table 3) indicate the number of pending cases at the end of the reporting years shown. At the end of 2021, 27 mediation cases were still pending from 2021, including eight suspended procedures (three from 2019, one from 2020, and four from the year under review). 14 cases had been completed by the time of going to press.

Processing time is expected to continue to increase, along with a growing number of cases – unjustified from a legal standpoint – in which the deadline is exceeded, resulting in more pending cases at the end of this year.

Table 3: Pending mediation procedures

End of 2021	**27 (14 completed by the time of going to press and 8 suspended)**
End of 2020	17 (9 completed by the time of going to press and 8 suspended)
End of 2019	43 (40 completed by the time of going to press and 3 suspended)
End of 2018	15 (13 completed in February 2019 and 2 suspended)



2.4 Legislative process

OFFICE CONSULTATION

Revision of the Intelligence Service Act

The Federal Act of 25 September 2015 on the Intelligence Service (IntelSA; SR 121) is in the process of being revised. The bill submitted to the FDPIC during the office consultation aimed to further extend the range of information to be excluded from the Freedom of Information Act.

Under the present Article 67 IntelSA, the Freedom of Information Act does not apply to access to official documents relating to information gathering under IntelSA. This term is clearly defined in Chapter 3 of the Intelligence Service Act. The revised article envisages excluding all intelligence information. In the FDPIC's view, by amending this article, the Federal Intelligence Service (FIS) is once again attempting to narrow the scope of the Freedom of Information Act by extending the range of information excluded from the Act. This new wording means that most of the FIS's activities will be removed from the purview of the Freedom of Information Act, contrary to the intention of the legislature, which introduced the Freedom of Information Act to promote transparency with regard to the purpose, organisation and activities of the Federal Administration.

The FDPIC strongly objected, among other things because the exceptions set out in Articles 7 to 9 FoIA – in particular the exceptions aimed at protecting the domestic and international security of Switzerland (Article 7 para. 1 let. c FoIA), the interests of Switzerland in matters of foreign policy (Article 7 para. 1 let. d FoIA) and privacy (Article 7 para. 2 FoIA) – are already in force and offer suitable and sufficient protection (s. Kap. 1.2).

Following the office consultation, after initially maintaining its position, the FIS eventually informed the FDPIC that it was abandoning the changes to the current Article 67 IntelSA.

The FDPIC

3.1 Duties and resources

The pandemic

The data processing projects designed to combat the pandemic – completed in a short time frame due to the health crisis – and the increased demand for public documents placed extraordinary pressure on staff again in the second year of the pandemic.

The FDPIC is a federal authority affiliated to the Federal Chancellery for administrative purposes, and as such he has implemented all the Federal Council's guidelines aimed at protecting employees during the pandemic. In February 2022, the Federal Council lifted the requirement for federal employees to work from home, and so on 1 March 2022 the FDPIC's staff were able to reduce work from home to the ordinary level agreed under the flexible working arrangement. Since then, people have been able to meet again face to face, which is particularly important for recruiting and supporting new staff.

Services and resources in the field of data protection

Number of staff

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

In its dispatch on the complete revision of the FADP, the Federal Council promised the FDPIC additional resources in the form of nine to ten staff positions (BBI 2017 7172). Switzerland's new Federal Act on Data Protection related to the Application of the Schengen Acquis in Criminal Matters (SDPA, SR 235.3) already covers an aspect of the complete revision. The Federal Council implemented this Act on 1 March 2019 and promised the FDPIC three additional staff positions to fulfil his new duties and powers. This increased the headcount to 27 FTEs in 2020. In view of the forthcoming entry into force of the revised FADP, originally scheduled for 2022, in spring 2021 the FDPIC asked the Federal Council to authorise the six remaining FTEs which had been approved as part of overall resource planning. When the new legislation comes into force, the Federal Council will only forward the FDPIC's new requests for resources to Parliament for a decision.

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

Table 4: Number of staff available for FADP concerns

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	**27**

Services

The FDPIC's duties as the data protection authority for the federal authorities and the private sector have been

divided into four service groups in line with the New Management Model (NMM) for the Federal Administration: consultancy, supervision, information and legislation. In the reporting year running from 1 April 2021 to 31 March 2022, the FDPIC's staff resources available for data protection were allocated to these four groups as follows:

Table 5: Services in data protection

Consultancy – private	22,1%	
Consultancy – Confederation	18,9%	
Cooperation with Cantons	1,4%	
Cooperation with authorities abroad	13,4%	
Total Consultancy		**55,8%**
Supervision	16,8%	
Certification	0,1%	
Data collection register	0,4%	
Total Supervision		**17,3%**
Information	13,1%	
Education, speeches and presentations	3,1%	
Total Information		**16,2%**
Legislation	10,7%	
Total Legislation		**10,7%**
Total date protection		**100,0%**

Consultancy

As set out in the opening section on 'Current challenges', the FDPIC still faces a consistently high demand for consultancy services as he is required to support large digital projects. During the year under review, the proportion of staff working in consultancy amounted to around 56%. In the FDPIC's inspection plan for 2022, seven large projects are currently receiving support in the form of consultancy. Six of these projects are related to the digital transformation of the Federal Administration ordered by the Federal Council, whereby the Federal Administration is doing its best to reduce the digitalisation backlog, largely brought about by the ongoing pandemic and widely reported by politicians and the media.

The FDPIC's resources remain tight for dealing with the legal and technological risks posed by the rapid pace of digitalisation. As a result, he was unable to provide timely support to the extent required to fully meet the increased demand for project consultancy again during the year under review. Over the course of the reporting period, three teams from the Data Protection Directorate responded to around 48 enquiries and complaints from members of the public each month with a standard letter referring the persons concerned to the option of civil proceedings. This is causing mounting confusion as the EU's General Data Protection Regulation requires EU data protection authorities to investigate all complaints from members of the public. Moreover, the new FADP also stipulates a more extensive obligation for the FDPIC to handle individual complaints from Swiss citizens directly.

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

Table 6: Consultancy for large-scale projects in 2021

Health/employment	3
Commerce and economy	3
Customs	1
Total	7

Supervision

The dynamics of cloud-based applications mean that inspections now have to be carried out quickly. The increasingly fast pace of work and the growing importance of combining technical and legal expertise mean that long interruptions to investigations

are no longer feasible, and several employees are required to manage more thorough inspections. Our current staffing levels severely limit the frequency of inspections. In 2018, around 12% of staff resources were used for supervisory duties, which was significantly below the long-term average of around 20%. In the last reporting periods, this proportion was at least prevented from falling below 15%. During the year under review, the proportion stood at 17.3%, around 2% higher. Our inspection plan for 2022 shows that 13 comprehensive inspections can be carried out with these resources. Compared with the volume of work carried out by the federal bodies and the number of large and medium-sized commercial enterprises (around 12,000) and foundations and associations (around 100 000) in Switzerland, the current frequency of inspections remains low. Explaining to the media and consumer protection organisations that the FDPIC's limited resources make him reluctant to open formal investigations remains a difficult task for the Commissioner. Public expectations in the run-up to the entry into force of the revised FADP are high, placing increasing pressure on the FDPIC.

Legislation

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

Complete revision of the FADP

In the run-up to the entry into force of the new FADP and the corresponding implementing ordinance, the FDPIC has extensive preparatory work in view of his new duties and powers and in order to inform people and companies in good time. The creation of three staff positions by the Federal Council with the entry into force of the new FADP has allowed the FDPIC to forge ahead with his work. In this regard, the Federal Council has also approved the remaining six staff positions for implementation of the FADP (see above).

Participation in committee consultations and parliamentary committee hearings

- During the year under review, the PIC-N invited us in April 2021 to discuss the easing of COVID restrictions for vaccinated persons. During the same month, the TTC-N consulted us on the revision of the Federal Act on the Surveillance of Post and Telecommunications (SPTA).
- At the end of October 2021 and in mid-January 2022, the PIC-N and the PIC-S invited us three times to discuss the revision of the Federal Act on Data Protection and its implementing ordinances.
- Also in October, the CDel sought our input on the presentation of a report on our practice in relation to Article 64 IntelSA.
- In November 2021, the PIC-N also sought our input on the 2022 budget and the 2023–2025 financial plan.
- At the end of the year under review, we were consulted twice by the SSHC-S on the Swisstransplant issue.
- Finally, in February 2022, the FDJP/FCh subcommittee of the CC-N carried out a half-day visit, which had to take place at the Federal Palace due to the pandemic.

Assessment criteria

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

This requires appropriate and sufficient resources in terms of staff, materials, technology and funds. The supervisory authority 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.

Services and resources in the field of freedom of information

The year under review was characterised not only by the ongoing pandemic but also by a surge in the number of mediation requests (see Section 2.2). This situation has once again shown that the 4.4 staff positions allocated to the Freedom of Information section are not sufficient for the performance of duties in accordance with the law. As mentioned above and contrary to the statements in its dispatch, the Federal Council has not yet approved any staff positions for the FDPIC to carry out his duties under the Freedom of Information Act.

Due to the pandemic and the measures taken by the Federal Council to protect public health, mediation sessions could not be held on site for several months in both the reporting year and the current year. As a result, the FDPIC had to revert to the written procedure during that time. This impacted negatively on the time needed to process individual procedures, causing a backlog. Furthermore, the growing number of mediation requests over the years and the increasing complexity of the requests mean that the FDPIC is exceeding the statutory 30-day time limit for completing procedures in an increasing number of cases.

The trend in the increase of mediation requests looks set to continue in 2022 and beyond, and the backlog is likely to make it increasingly difficult to process new cases within the statutory time limit with the currently available resources. This means that the swift handling of procedures envisaged by the legislator can no longer be guaranteed.

As regards freedom of information, it is again up to the political authorities to decide whether and to what extent the FDPIC is to be allocated resources to fulfil his mediation and consultancy duties.

Regarding the individual service groups, resources are to be allocated based on the following outcome objectives (see Table 7):

Table 7: Outcome objectives FDPIC

Service group	Outcome objectives
Consultancy	The consultancy that the FDPIC provides for individuals and for businesses and federal authorities running projects involving sensitive data meets general expectations. The FDPIC uses tools appropriate to the digital world.
Supervision	The frequency of FDPIC inspections is credible.
Information	The FDPIC proactively raises public awareness of the risks posed by individual digital technologies and their usage. He has a contemporary, user-friendly website. Reports can be sent to the FDPIC at any time via a secure, user-friendly reporting portal.
Legislation	The FDPIC has an early say on and actively influences all special rules and regulations created at national and international level. He helps the parties involved to formulate rules of good practice.

3.2 Communication

Main focus areas of our communication activities

Pandemic-related topics, which dominated the last reporting period, continued to take centre stage during the year under review. However, the enquiries received by the FDPIC focused less on contact tracing and more on the design and use of the COVID certificate and the associated app. The FDPIC and his experts had their work cut out again in communication on these issues. We successfully pushed for a data-minimised "light certificate" containing no health data. Another topic was the vaccination registration platform myvaccines.ch, which the operators closed down due to security issues. Overall, the main focus of our communication activities was on COVID-related issues.

Another focus of attention was data leakage in various sectors, often exposed by investigative journalist networks. Targets included social networks and high-public-interest websites such as public transport, organ donation and breast implant websites. We also received a large number of reports of attacks on company systems. As a result, we are working more closely with the National Cyber Security Centre (NCSC). The reporting of data leaks to the FDPIC will become mandatory under the new Federal Act on Data Protection (see Focus I).

Surveillance remains a subject of discussion, be it in the workplace or in private areas such as retail commerce or via state spyware. Subjects such as tracking (mobility, internet or consumer behaviour) and the development of biometric recognition systems that use algorithms to spy on citizens (e. g. Clearview) remain hot topics that will continue to attract media interest. Data protection remains a key issue in the numerous digital transformation projects of the Federal Administration and in the private sector.

During the year under review, the FDPIC and his communications team handled a total of around 550 enquiries from the media and other organisations.

Greater media and public awareness

In our media monitoring (covering a selection of Swiss media and key international printed publications), we recorded more than 6,000 posts compared with around 4,000 last year. This confirms the trend observed in terms of increasing interest in the topic of data protection and informational self-determination and increasing media coverage. Overall, media coverage of COVID-related issues was slightly lower but still accounted for around one-third of all articles. Journalists also focused on surveillance, data

disclosure and regulatory issues relating to the tech giants (GAFAM), cloud computing, cyber security, artificial intelligence and big data.

Furthermore, there was a noticeable increase in the number of reports based on documents obtained under the Freedom of Information Act.

Our authority also received an increased number of enquiries and concerns from businesses and members of the public. We handled approximately 6,600 enquiries addressed to us by email, post or via our hotline (compared with 4,200 during the last reporting year).

The FDPIC attended around fifty events, slightly more than last year. On International Data Protection Day at the end of January 2022, he attended the public conference hosted by the University of Lausanne. In his keynote speech, the FDPIC stressed that data protection authorities were working to ensure that digital transformation took place in strict compliance with individuals' fundamental right to a private and self-determined life.

Annual report and new website

At the end of the reporting year, the Communications department employed 2.6 full-time equivalents, shared among three persons. The same priority is given to media work as to the annual report project. The 28th annual report for 2020/2021 was published on 29 June 2021 in accordance with Article 30 FADP. The report was produced and printed again in four languages and is also available on our website as an epaper and as a freely accessible PDF document.

In autumn 2021, we also launched our website redesign project. Following a tender process, we began the design phase in 2022 working together with an external agency. Our aim is to simplify the website, which has grown over many years, and to update the content in order to provide users with a contemporary, user-friendly portal tailored to their needs. The FDPIC's new website will take into account the provisions of the new FADP and will go live before the new act becomes effective.

Opinions and recommendations

During the year under review, the FDPIC published various opinions and statements on current projects and events, including on the following topics:

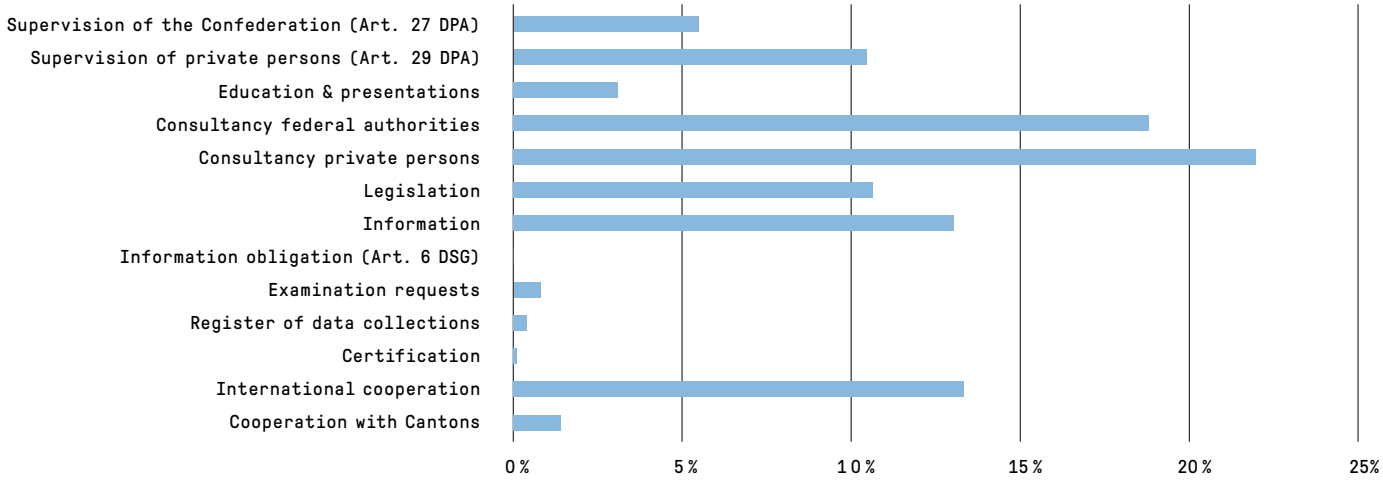
- Case investigations into the SocialPass app and the myvaccines.ch and Swisstransplant platforms
- Suspected unauthorised surveillance of individuals (Mitto AG)
- Monitoring of the development of the COVID vaccine certificate and the data-minimised light version
- Data transfer to foreign countries
- Non FADP-compliant sharing of data by the Swiss shooting club
- Various data leaks including via social networks

We published 45 recommendations on our website regarding access to documents of the Federal Administration under the Freedom of Information Act (compared with 26 recommendations in 2020).

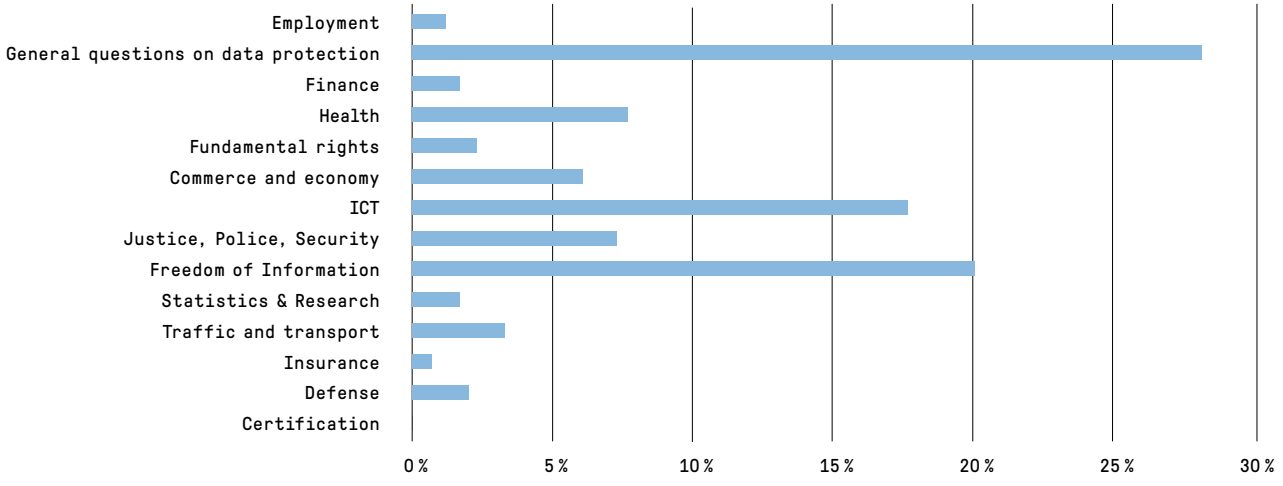
3.3 Statistics

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

Workload per tasks

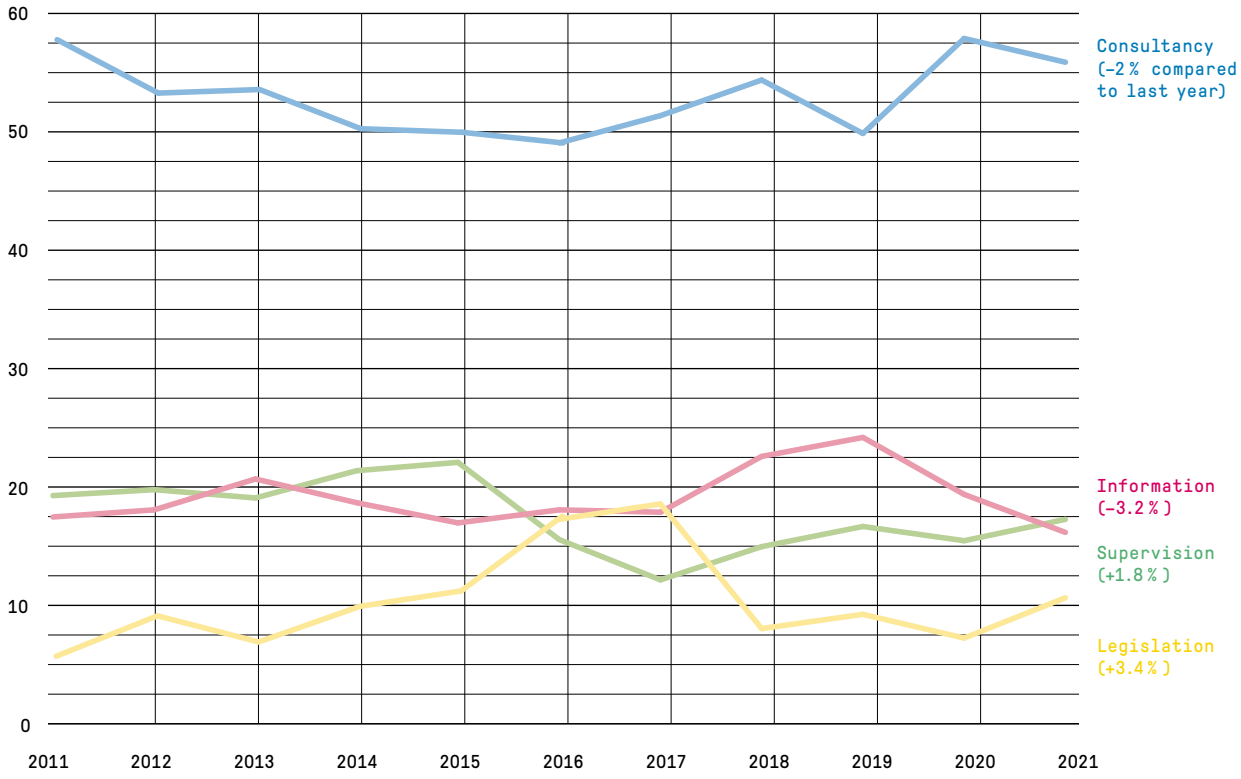


Workload per material



Multi-year comparison

(as a percentage)



Overview of applications from 1st January to 31 December 2021

Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No document available
FCh	57	26	8	9	2	5	7
FDFA	156	77	15	47	2	5	10
FDHA	422	168	25	139	21	38	31
FDJP	103	46	18	13	1	2	23
DDPS	281	203	11	38	7	3	19
FDF	119	54	22	21	6	9	7
EAER	92	48	13	22	2	6	1
DETEC	146	71	10	35	6	10	14
OAG	8	0	4	0	1	0	3
PS	1	1	0	0	0	0	0
Total 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (3)	78 (7)	115 (8)
Total 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Total 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Total 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Total 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	–
Total 2016 (%)	558 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	–
Total 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	–
Total 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	–
Total 2013 (%)	461 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	–
Total 2012 (%)	522 (100)	230 (44)	140 (27)	123 (24)	19 (4)	6 (1)	–
Total 2011 (%)	481 (100)	206 (44)	127 (27)	128 (27)	0 (0)	9 (2)	–

Statistics on applications for access under the Freedom of Information Act from 1st January to 31 December 2021

	Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Federal Chancellery FCh	FCh	**41**	19	6	7	2	0	7
	FDPIC	**16**	7	2	2	0	5	0
	Total	**57**	**26**	**8**	**9**	**2**	**5**	**7**
Federal Departement of Foreign Affairs FDFA	FDFA	**156**	77	15	47	2	5	10
	Total	**156**	**77**	**15**	**47**	**2**	**5**	**10**
Federal Departement of Home Affairs FDHA	GS FDHA	**13**	8	0	2	0	2	1
	FOGE	**24**	20	0	0	1	0	3
	FOC	**1**	0	1	0	0	0	0
	SFA	**1**	1	0	0	0	0	0
	METEO CH	**0**	0	0	0	0	0	0
	NL	**0**	0	0	0	0	0	0
	FOPH	**251**	90	11	101	6	27	16
	FOS	**12**	8	3	0	0	0	1
	FSIO	**13**	8	3	1	0	0	1
	compenswiss	**2**	1	1	0	0	0	0
	FSVO	**28**	17	1	9	1	0	0
	SNM	**0**	0	0	0	0	0	0
	SWISS MEDIC	**72**	15	3	26	11	8	9
	SUVA	**5**	0	2	0	2	1	0
	Total	**422**	**168**	**25**	**139**	**21**	**38**	**31**
Federal Department of Justice and Police FDJP	GS FDJP	**14**	7	0	1	0	1	5
	FOJ	**38**	13	10	0	0	0	15
	FEDPOL	**14**	10	3	1	0	0	0
	METAS	**1**	1	0	0	0	0	0
	SEM	**24**	10	2	9	1	0	2
	PTSS	**3**	0	0	2	0	0	1
	SIR	**5**	2	3	0	0	0	0
	IPI	**2**	2	0	0	0	0	0
	FGB	**0**	0	0	0	0	0	0
	ESchK	**1**	1	0	0	0	0	0
	FAOA	**0**	0	0	0	0	0	0
	ISC	**0**	0	0	0	0	0	0
	NKVF	**1**	0	0	0	0	1	0
	Total	**103**	**46**	**18**	**13**	**1**	**2**	**23**

	Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Federal Department of Defence, Civil Protection and Sport DDPS	GS DDPS	**27**	10	0	8	0	1	8
	Defence	**29**	17	1	7	3	1	0
	FIS	**28**	0	6	15	0	0	7
	armasuisse	**12**	3	4	3	0	1	1
	FOSPO	**172**	170	0	0	2	0	0
	FOCP	**8**	1	0	5	0	0	2
	swisstopo	**5**	2	0	0	2	0	1
	OA	**0**	0	0	0	0	0	0
	Total	**281**	**203**	**11**	**38**	**7**	**3**	**19**
Federal Departmemt of Finance FDF	GS FDF	**25**	8	6	7	0	2	2
	FITSU [1]	**0**	0	0	0	0	0	0
	FFA	**7**	2	0	3	0	0	2
	FOPER	**4**	4	0	0	0	0	0
	FTA	**14**	4	7	3	0	0	0
	FCA [2]	**42**	22	3	7	4	6	0
	FOBL	**5**	3	1	0	1	0	0
	FOITT	**7**	5	0	0	1	0	1
	SFAO	**9**	1	4	1	0	1	2
	SIF	**3**	3	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	CCO	**3**	2	1	0	0	0	0
	Total	**119**	**54**	**22**	**21**	**6**	**9**	**7**

[1] **Since 1.1.2021 at FCh DTI**

[2] **Since 1.1.2022 FOCBS**

	Department	Number of requests	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	**6**	6	0	0	0	0	0
	SECO	**28**	18	3	4	2	1	0
	SERI	**13**	10	2	0	0	0	1
	FOAG	**13**	3	1	8	0	1	0
	Agroscope	**3**	2	0	1	0	0	0
	FONES	**2**	1	1	0	0	0	0
	FHO	**1**	0	0	1	0	0	0
	PUE	**4**	1	3	0	0	0	0
	COMCO	**10**	4	1	3	0	2	0
	ZIVI	**0**	0	0	0	0	0	0
	FCAB	**1**	0	0	0	0	1	0
	SNSF	**0**	0	0	0	0	0	0
	SFIVET	**1**	0	1	0	0	0	0
	ETH Board	**9**	2	1	5	0	1	0
	Innosuisse	**1**	1	0	0	0	0	0
	Total	**92**	**48**	**13**	**22**	**2**	**6**	**1**
Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	**12**	8	1	0	0	1	2
	FOT	**7**	3	0	2	0	1	1
	FOCA	**10**	6	1	1	1	1	0
	SFOE	**11**	3	3	3	0	1	1
	FEDRO	**6**	5	0	1	0	0	0
	OFCOM	**23**	9	0	11	0	1	2
	FOEN	**64**	34	4	15	3	1	7
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	ENSI	**9**	2	0	1	2	3	1
	PostCom	**3**	1	0	1	0	1	0
	ICA	**1**	0	1	0	0	0	0
	Total	**146**	**71**	**10**	**35**	**6**	**10**	**14**
Office of the Attorney General OAG	OAG	**8**	0	4	0	1	0	3
	Total	**8**	**0**	**4**	**0**	**1**	**0**	**3**
Parliamentary Services PS	PS	**1**	1	0	0	0	0	0
	Total	**1**	**1**	**0**	**0**	**0**	**0**	**0**
	Total sum	**1385**	**694**	**126**	**324**	**48**	**78**	**115**

Requests for access 2021 with Corona reference

	Department	Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/ suspended	Request withdrawn	Pending requests	No dcument available
Federal Chancellery FCh	FCh	**5**	3	1	1	0	0	0
	FDPIC	**0**	0	0	0	0	0	0
	Total	**5**	**3**	**1**	**1**	**0**	**0**	**0**
Federal Departement of Foreign Affairs FDFA	FDFA	0	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Federal Departement of Home Affairs FDHA	GS FDHA	**6**	5	0	0	0	1	0
	FOGE	**0**	0	0	0	0	0	0
	FOC	**0**	0	0	0	0	0	0
	SFA	**0**	0	0	0	0	0	0
	METEO CH	**0**	0	0	0	0	0	0
	NL	**0**	0	0	0	0	0	0
	FOPH	**217**	82	2	93	4	20	16
	FOS	**0**	0	0	0	0	0	0
	FSIO	**1**	1	0	0	0	0	0
	compenswiss	**0**	0	0	0	0	0	0
	FSVO	**0**	0	0	0	0	0	0
	SNM	**0**	0	0	0	0	0	0
	SWISS MEDIC	**41**	6	2	17	6	6	4
	SUVA	**1**	0	0	0	1	0	0
	Total	**266**	**94**	**4**	**110**	**11**	**27**	**20**
Federal Departmemt of Finance FDF	GS FDF	**5**	0	4	1	0	0	0
	FITSU [1]	**0**	0	0	0	0	0	0
	FFA	**6**	1	0	3	0	0	2
	FOPER	**0**	0	0	0	0	0	0
	FTA	**1**	0	1	0	0	0	0
	FCA [2]	**2**	0	0	2	0	0	0
	FOBL	**1**	0	0	0	1	0	0
	FOITT	**6**	3	0	1	1	0	1
	SFAO	**1**	0	0	0	0	1	0
	SIF	**0**	0	0	0	0	0	0
	PUBLICA	**0**	0	0	0	0	0	0
	CCO	**0**	0	0	0	0	0	0
	Total	**22**	**4**	**5**	**7**	**2**	**1**	**3**

[1] **Since 1.1.2021 at FCh DTI**

[2] **Since 1.1.2022 FOCBS**

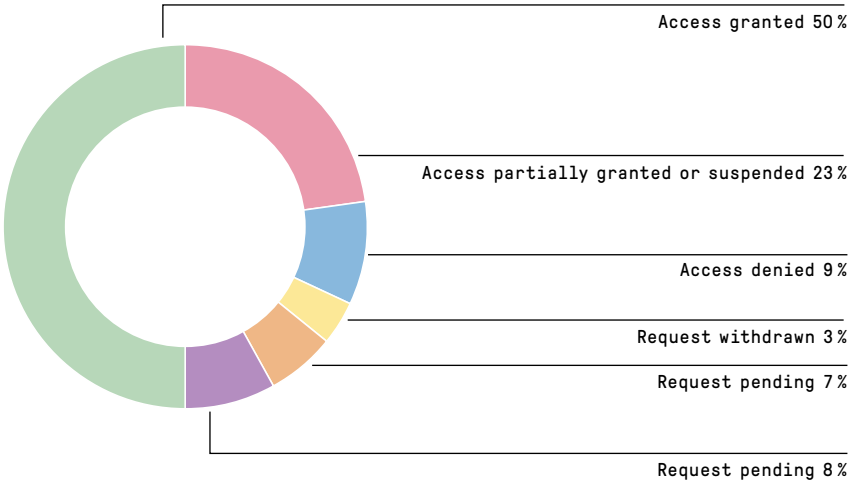
	Department	Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/ suspended	Request withdrawn	Pending requests	No dcument available
Federal Department of Justice and Police FDJP	GS FDJP	**1**	1	0	0	0	0	0
	FOJ	**0**	0	0	0	0	0	0
	FEDPOL	**0**	0	0	0	0	0	0
	METAS	**0**	0	0	0	0	0	0
	SEM	**0**	0	0	0	0	0	0
	PTSS	**0**	0	0	0	0	0	0
	SIR	**0**	0	0	0	0	0	0
	IPI	**0**	0	0	0	0	0	0
	FGB	**0**	0	0	0	0	0	0
	ESchK	**0**	0	0	0	0	0	0
	FAOA	**0**	0	0	0	0	0	0
	ISC	**0**	0	0	0	0	0	0
	NKVF	**0**	0	0	0	0	0	0
	Total	**1**	**1**	**0**	**0**	**0**	**0**	**0**
Federal Department of the Environment, Transport, Energy and Communications DETEC	GS DETEC	**0**	0	0	0	0	0	0
	FOT	**0**	0	0	0	0	0	0
	FOCA	**1**	0	0	1	0	0	0
	SFOE	**0**	0	0	0	0	0	0
	FEDRO	**0**	0	0	0	0	0	0
	OFCOM	**1**	0	0	1	0	0	0
	FOEN	**0**	0	0	0	0	0	0
	ARE	**0**	0	0	0	0	0	0
	ComCom	**0**	0	0	0	0	0	0
	ENSI	**0**	0	0	0	0	0	0
	PostCom	**0**	0	0	0	0	0	0
	ICA	**0**	0	0	0	0	0	0
	Total	**2**	**0**	**0**	**2**	**0**	**0**	**0**
Federal Department of Defence, Civil Protection and Sport DDPS	GS DDPS	**0**	0	0	0	0	0	0
	Defence/Army	**25**	15	1	5	3	1	0
	FIS	**0**	0	0	0	0	0	0
	armasuisse	**0**	0	0	0	0	0	0
	FOSPO	**4**	2	0	0	2	0	0
	FOCP	**1**	0	0	1	0	0	0
	swisstopo	**0**	0	0	0	0	0	0
	OA	**0**	0	0	0	0	0	0
	Total	**30**	**17**	**1**	**6**	**5**	**1**	**0**

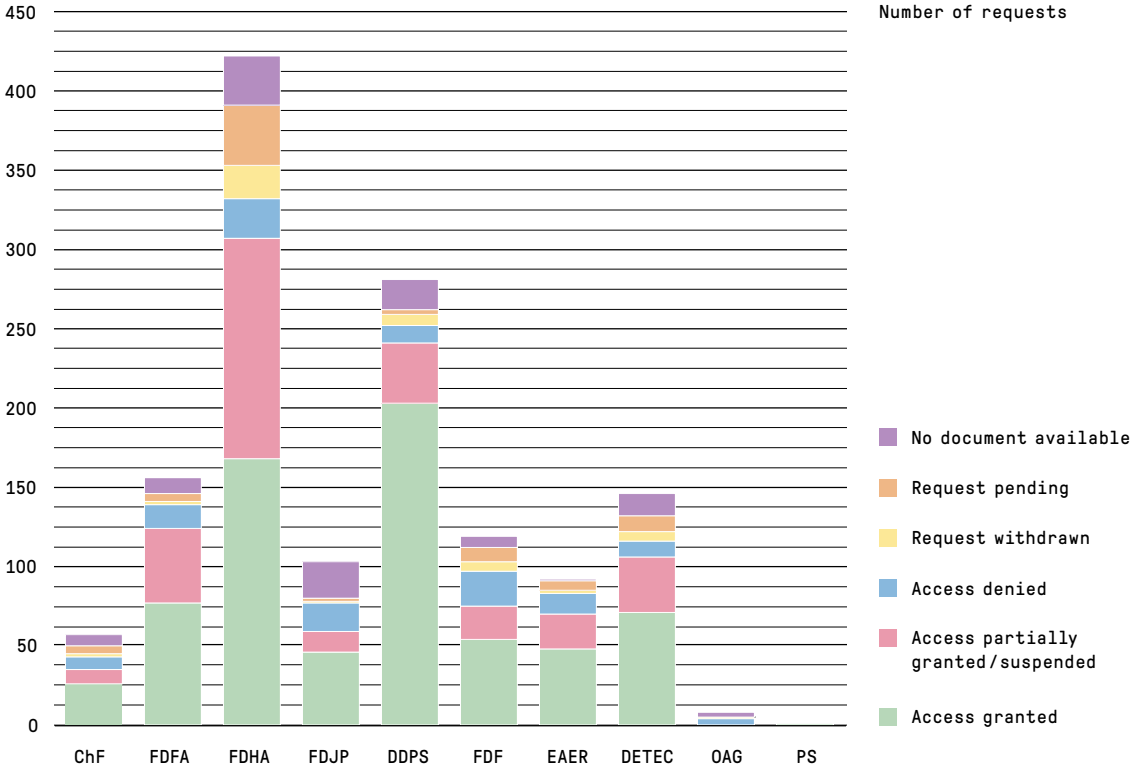
	Department	Requests with Corona reference	Access completely granted	Access completely denied	Access partially granted/suspended	Request withdrawn	Pending requests	No dcument available
Federal Department of Economic Affairs, Education and Research EAER	GS EAER	**1**	1	0	0	0	0	0
	SECO	**5**	1	1	3	0	0	0
	SERI	**1**	0	0	0	0	0	1
	FOAG	**0**	0	0	0	0	0	0
	Agroscope	**0**	0	0	0	0	0	0
	FONES	**0**	0	0	0	0	0	0
	FHO	**0**	0	0	0	0	0	0
	PUE	**0**	0	0	0	0	0	0
	COMCO	**0**	0	0	0	0	0	0
	ZIVI	**0**	0	0	0	0	0	0
	FCAB	**0**	0	0	0	0	0	0
	SNSF	**0**	0	0	0	0	0	0
	SFIVET	**0**	0	0	0	0	0	0
	ETH Board	**3**	0	1	2	0	0	0
	Innosuisse	**0**	0	0	0	0	0	0
	Total	**10**	**2**	**2**	**5**	**0**	**0**	**1**
Office of the Attorney General OAG	OAG	**0**	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Parliamentary Services PS	PS	**0**	0	0	0	0	0	0
	Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**
	Total sum	**336**	**121**	**13**	**131**	**18**	**29**	**24**

Number of requests for mediation by category of applicant

Category of applicant	2021	2020	2019	2018	2017
Media	53	31	34	24	21
Private individuals (or no exact assignment possible)	49	42	40	26	35
Stakeholders (associations, organisations, clubs etc.)	16	5	7	9	14
Lawyers	12	7	5	4	2
Companies	19	7	47	13	7
Universities	0	1			
Total	**149**	**93**	**133**	**76**	**79**

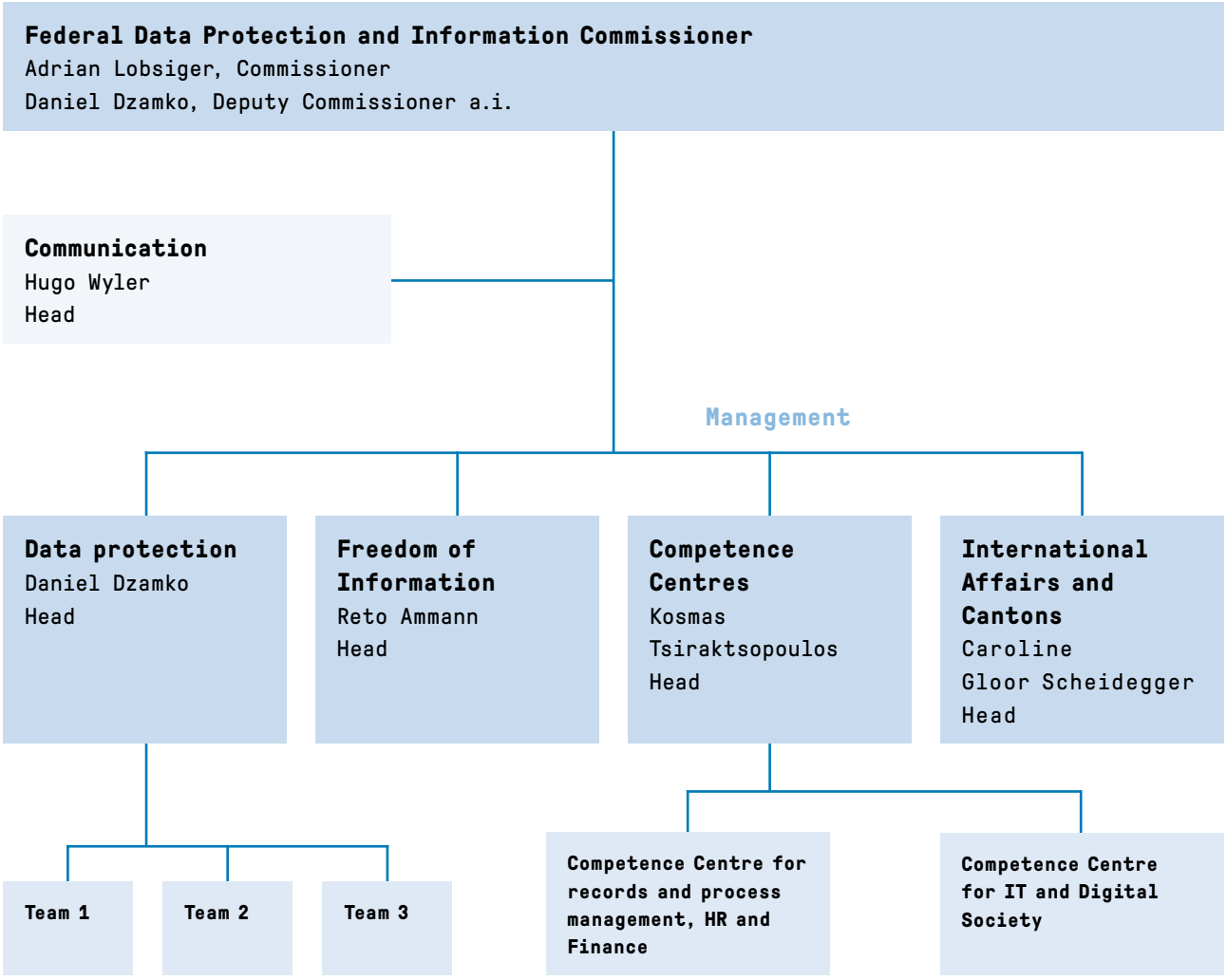
Applications for access in the federal administration from 1st January to 31 December 2021





3.4 Organisation FDPIC (Status 31 March 2022)

Organisation chart



Employees of the FDPIC

Number of employees	39		
FTE	32.4		
per gender	Women	19	49 %
	Men	20	51 %
by employment level	1–89 %	27	69 %
	90–100 %	12	31 %
by language	German	29	77 %
	French	8	20 %
	Italian	1	3 %
by age	20–49 years	23	59 %
	50–65 years	16	41 %
Management	Women	3	33 %
	Men	6	67 %

Abbreviations

AI Artificial intelligence

CJEU Court of Justice of the European Union

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

DaziT Transformation programme of the FOCBS

DPCO Ordinance on Data Protection Certification

DPIA Data Protection Impact Assessment

DPO Ordinance to the Federal Act on Data Protection

DTI Digital Transformation and ICT Steering Sector of the Federal Chancellery

E-ID Electronic Identity

EDPB European Data Protection Board

EDPS European Data Protection Supervisor

EPR Electronic Patient Record

EPRA Federal Act on the Electronic Patient Record

FADP Federal Act on Data Protection

Fedpol Federal Office of Police

FIS Federal Intelligence Service

FOCBS Federal Office for Customs and Border Security

FoIA Freedom of Information Act

GDPR General Data Protection Regulation

GPA Global Privacy Assembly

ICT Information and Communication Technology

MDA Mobility Data Agency

MODIG Federal Mobility Data Infrastructure Act

NaDB National data management programme

NaDIM National Mobility Data Infrastructure

NCSC National Cyber Security Centre

OECD Organisation for Economic Co-operation and Development

PNR Passenger Name Records

PRA Federal Act on Political Rights

Privatim Association of Swiss Commissioners for Data Protection

SAS Swiss Accreditation Service

SCC Standard Contractual Clauses

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

SEC U.S. Securities and Exchange Commission

Figures and tables

Figures

Tables

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. 410.029.ENG

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

Key figures

Workload data protection

55,8 % Consultancy

17,3 % Supervision

16,2 % Information

10,7 % Legislation

Applications for access Freedom of Information (FoIA)

50 % granted

23 % partially granted or suspended

9 % denied

4 % withdrawn

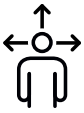
6 % pending

8 % no document available

Data protection concerns

Fair information

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



Freedom of Choice

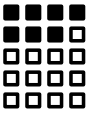
Those affected from data processing (data subjects) give their consent on the basis of transparent information and are provided with genuine freedom of choice.

Risk analysis

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

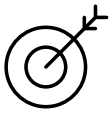
Data correctness

The processing takes place with applicable data.



Proportionality

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



Purpose

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

Data security

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

Documentation

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

Responsibility

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

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

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