25 June 2018

Summary of main issues in the 25th annual report

Data protection

On 15 September 2017 the Federal Council approved the Dispatch on the **Total Revision of the Federal Act on Data Protection** and amendments to other data protection legislation for debate in Parliament. The intention behind the revision is to improve data protection, in particular by increasing data processing transparency and by giving data subjects better control over their own data. While we welcomed the basic tenets of the revision, we expressed some reservations over the Federal Council's draft law relating to terminological and material **divergences from the EU's General Data Protection Regulation (GDPR)** and from the modernised Convention 108. These differences make the legal situation for those Swiss companies and authorities directly affected by the GDPR more complex, and create legal uncertainty. Furthermore, we urged in vain that the project should be adopted quickly (Section 1.1.1).

The Federal Council charged the Federal Department of Home Affairs (FDHA) with drafting legislation on making it easier for all federal, cantonal and communal authorities, not only the social insurance authorities, to **use OASI numbers as personal identifiers**. At the end of September 2017, ETH professor David Basin was invited by the FDPIC and the Federal Office of Justice (FOJ) to present an analysis of risks inherent in data protection law with regard to the use of personal identifiers and in plans to extend the use of AHVN13 (Section 1.1.2).

With federal elections approaching in 2019, the FDPIC published on its website some explanations about data protection laws and the **use of digital campaigning tools**. Using these tools, political groups and interest groups can organise personal contacts digitally and identify interaction between them. They can also integrate specific activities into the websites used by the contacts. We pointed out that data subjects must be given clear and complete information about this type of data processing, and that a person must give their free and express consent on the basis of this information before their data can be used (Section 1.1.3).

The SBB informed us about several projects involving data protection. These include the use of **bodycams** and the development of new apps. The SBB's own data protection officer conducted an initial data protection analysis of these projects. In the case of the **Swiss Pass Mobile app**, the FDPIC indicated that all passengers wishing to travel in anonymity should be able to do so (Section 1.2.1).

In late December 2017 Swisscom informed the FDPIC that the contact data of around 800,000 of its customers had been accessed illegally the previous autumn. We advised Swisscom on minimising risk and safeguarding their clients' rights to information. Once the facts of the matter had been established, the necessary protections introduced and the clients informed of the **data leak**, the FDPIC was able to conclude the matter without undertaking any formal measures (Section 1.3.2).

The primary objective of introducing **electronic identity verification (E-ID)** is to increase legal certainty in the digital field. We followed this major project during the consultation procedure on the basic legislation and also in two private initiatives (Section 1.3.3).

Feldeggweg 1, 3003 Bern
Tel. 058 464 94 10
www.edoeb.admin.ch

The Federal Supreme Court supported the FDPIC's position on the **right to information on telecommunications metadata**. When information is requested, telecommunications providers must be able to provide all information which relates to the person in question, or which can be assigned to them (Section 1.3.4).

The FDPIC had strongly differing views from fedpol regarding the Federal Act on Police **Counterterrorism Measures**. Federal police law is regulated in a number of pieces of legislation, making it difficult to maintain an overview of the different ways in which personal data is processed. The new draft law complicates the situation even further. We therefore propose that a law on the activities of federal police bodies be drawn up, similar to existing cantonal laws. There must be a clear regulation on the information system in which data on police counterterrorism measures are processed (Section 1.4.3).

The FDPIC reviewed data processing relating to **Schengen visas** at the State Secretariat for Migration (SEM), end-user of the Schengen Information System (SIS). In accordance with the Schengen Association Agreements, the FDPIC conducted a control at the SEM premises of alerts for the purposes of refusing entry or permission to stay (Sections 1.4.6 and 1.4.7).

In early 2018 the **third Schengen evaluation** of Switzerland as an associated member was carried out. This concerns all areas of cooperation under Schengen: management of external borders (airports), return/repatriation, the Schengen Information System SIS II/SIRENE, joint policy on visas, police cooperation and the processing of personal data. The work was coordinated by the Federal Office of Justice (FOJ) in conjunction with the Directorate for European Affairs (DEA). The FDPIC advised on data protection issues (Section 1.4.5).

The FDPIC investigated a case in the **medical insurance** field, where there is a **trend towards outsourcing** tasks to service providers outside the industry. In this incident, a contractor opened the correspondence between an insured person and their medical insurer and processed the information therein (Section 1.6.3). We urged the service provider Swisscom Health and the Ärztekasse to provide patients with clearer information about outsourcing on their websites (Section 1.5.3).

Several medical insurers offer their clients **health apps and bonus programmes**. We looked at whether insured persons voluntarily provide their insurers with their health data, and whether data protection and data security regulations are respected. The FDPIC conducted a review of the Helsana+ medical insurance bonus programme and established that the legal basis required by the Data Protection Act was missing from this. The FDPIC therefore recommended that Helsana Zusatzversicherungen AG refrain from processing data relating to compulsory health insurance, and subsequently took legal action in the Federal Administrative Court (Section 1.6.4).

In the restaurant and catering trade, businesses are increasingly using **biometric time-tracking and access systems** (e.g. time logging via fingerprint). As this data is sensitive, its use should be restricted (Section 1.7.4). It seems that navigation devices in company vehicles and other **devices with GPS** are increasingly being used to monitor workers. We received several queries from persons affected in 2017. This type of monitoring is only permitted if both data protection laws and employment laws are complied with (Section 1.7.3). In the interests of transparency and in order to avoid disputes during and after an employment, employers should establish **guidelines on how staff should use IT** and define all obligations and rights (Section 1.7.2).

Since April 2017, US companies can self-certify for the **Swiss-US Privacy Shield**, which guarantees them an appropriate level of data protection. In the year under review, the FDPIC monitored the implementation of the Privacy Shield and published a **guide** for the public. This guide explains the certified companies' obligations and the rights of data subjects, and what the latter can do if they have a complaint. In autumn 2018 the first assessment of the Swiss-US Privacy Shield will be conducted, parallel to the second assessment of the EU-US Privacy Shield (Sections 1.8.1 and 3.2).

The FDPIC opened an investigation into the **data leak at the debt collection company EOS Schweiz AG**, which affected patients of Swiss doctors and dentists in particular. In a public statement we drew attention to the fact that medical personnel may only pass on to third parties patients' data which is actually required for invoicing or debt collection. Medical personnel are liable to prosecution if they pass on patients' health data to third parties without good cause (Section 1.8.2).

The advertising company APG/SGA asked us to provide a data protection appraisal of a platform for **personalised advertising in apps based on location data**. Because this allows extensive movement profiles and location data to be processed for an indefinite period of time, and it is relatively easy to identify the data subjects in many cases, the FDPIC proposed some specific measures. Users must also be clearly informed about the data processing when installing apps from third-party providers. They must give their express consent to their data being processed and must be able to withdraw this consent at any time (Section 1.8.4).

The FDPIC was in contact with the **advertising marketer Admeira**, whose portfolio includes Ringier, SRG and Swisscom. Data subjects should be able to object to their personal data being passed on for advertising purposes. The FDPIC advised Swisscom on its duty to provide information to its customers regarding its new data protection regulations. Data subjects must be made aware of data flows and processing in all cases (Section 1.8.5).

New standards on the global prevention of tax fraud and tax evasion are being implemented over a wider area. As part of the recently introduced **automatic exchange of information over financial accounts** (AIEO), Switzerland has been gathering data since 2017 and this will be exchanged in a first instance in 2018. In 2016 the Federal Assembly agreed the introduction of the AIEO with a first series of countries, including the EU member states. In June 2017 the Federal Council issued the Dispatch on the Introduction of the AIEO with a further 41 countries. The FDPIC indicated that more than 30 of these countries do not have an adequate level of data protection, meaning that additional data protection guarantees are necessary (Section 1.9.1).

Prospective tenants must often provide a lot of personal information to potential landlords on **application forms to rent apartments**. We explain on our website what information may be asked for on such forms and which questions must be omitted from the point of view of data protection (Section 3.2).

The provisions of the **EU General Data Protection Regulation (GDPR)** are in many cases directly applicable to Swiss businesses which process the data of EU citizens or offer services in the EU. We published detailed information on this on our website, and have drawn up a comprehensive **guide** on the new obligations for businesses and the privacy protection rights of private individuals (Section 3.2).

Freedom of information

In 2017 the FDPIC ran a pilot scheme to **speed up the arbitration procedure** and to work through the backlog of cases. The evaluation report shows that the objectives were achieved with the measures

taken and the pilot scheme was a success. In view of the positive results, the scheme is now made part of normal operations (Section 2.3.1).

The draft ordinance on the new Intelligence Service Act originally contained a provision which would have excluded virtually all **Federal Intelligence Service** documents. This provision, which we criticised, was then removed following the consultation procedure (Section 2.4.1).

In the previous reporting period, the FDPIC objected to restrictions on the freedom of information in the draft document on the **Organisation of Railway Infrastructure** (Section 2.3.1 of the 24th annual report). The Federal Supreme Court ruled that the list of risks and faults in public transport in a Federal Office of Transport (FOT) database must be made publicly available, and rejected the appeal by the FOT, which did not want to give a journalist access to this list (Section 2.4.2 of this report). At the end of May Parliament decided to exclude the FOT's supervisory activities in the security field from the Freedom of Information Act.

The full annual report is available online in German and French (www.derbeauftragte.ch – Dokumentation) or the print version can be ordered from FOBL, Publications distribution, 3003 Bern: Art. No 410.025.d/f Orders online: http://www.bundespublikationen.admin.ch