



1 July 2013

## Summary of a selection of topics covered in the 20th Report on Activities

### General data protection issues

Judging by the number of inquiries sent by citizens to the FDPIC, operators of **leisure centres** seem to be making increasing use of video cameras to **supervise sensitive areas such as changing rooms and toilets**. From a data protection perspective, this is an extremely worrying development since it constitutes a clear encroachment on the privacy of the persons concerned. The FDPIC has published his comments on the situation (Section 1.2.1).

Many Swiss **ski resorts** have installed an **access control system**, but the security of the data needs to be improved. The system manufacturer has agreed to **introduce the technical improvements** demanded by the FDPIC as a **matter of urgency** (Section 1.2.2).

The FDPIC carried out an **inspection** on the **Swiss Federal Railways database** containing information on **travellers caught without a valid ticket**. He concluded that a **formal legal basis** needed to be created for the information system. The Federal Office of Transport has said it would take the necessary steps to start the legislative process. At the time when the inspection was carried out, Swiss Federal Railways had not yet implemented the planned deletion of data in their IT system. The FDPIC is currently in the process of verifying the data deletion model and its implementation (Section 1.2.3).

The adoption of the Federal Act on the Promotion of Gymnastics and Sport established a legal basis for the **transmission of data to the World Anti Doping Agency**. However, as in this particular case the data have to be transferred abroad, it is imperative that a **contractual agreement** be signed to ensure a **satisfactory level of data protection** (Section 1.2.6).

### Internet

**Naming and shaming individuals** on the internet is becoming an increasingly popular sport: customers who don't pay their bills, officials who reject an applicant's request, or simply persons with a particular political view, may find their names published on an **Internet blacklist** so that they can be exposed to public opprobrium. However, the publication of names on the Internet generally unlawfully breaches the **privacy rights of the person involved** (Section 1.3.1).

The ruling of the **Federal Supreme Court** in the **Logistep** case has created a degree of uncertainty as to whether, under current legislation, it is still possible to **prosecute individuals who infringe copyright law**. Efforts are now being made to introduce measures that facilitate the **legal enforcement of copyright on the Internet** and thus to create clarity in the matter (Section 1.3.3).



**Businesses** and **public authorities** are becoming increasingly interested in learning about how best to market themselves through the **social media**. This has led to the creation of **social media monitoring** services. These services rely on the processing of **personal data**, which in turn means that the principles of data protection must be respected (Section 1.3.5).

### **Justice, Police, Security**

In October 2012 the FDPIC participated for the first time in a **Schengen data protection evaluation**. A small team of experts evaluated the **three Baltic states**. The experiences gained during this process will be useful for the evaluation of Switzerland, which is due to take place soon (Section 1.4.1).

Switzerland and the USA have signed the PCSC agreement (Preventing and Combating Serious Crime) allowing the **exchange of fingerprints and DNA data**, and the HSPD-6 memorandum of understanding on **exchanging intelligence on persons suspected or known to be engaged in terrorist activities**. This allows Switzerland to remain in the **US Visa Waiver Program**. Both agreements include data protection rules (Section 1.4.4).

Within the framework of interministerial consultations, the FDPIC has published his opinion on the draft revision of the federal law on the **monitoring of postal and telecommunications traffic**. A **legal basis** will now be established for the use of **computer programmes**. The FDPIC had demanded that a similar basis be created for the publication of data in conjunction with services that are provided over telecommunication networks (Section 1.4.5).

The Swiss government has launched a second consultation procedure for its **draft Intelligence Agency Act**. The new version includes **various improvements in the area of data protection**. However, there are still many unresolved **issues**, particularly in regard to intelligence gathering operations or the **exclusion of the Swiss intelligence services** from the application of the **Freedom of Information Act** (Section 1.4.6).

The FDPIC has inspected the **automatic vehicle search and traffic control system** operated by the **Swiss Customs Authorities**, and can confirm that it rests on an adequate legal basis. The Federal Office of Police provides an **index** of vehicle license plates contained in the RIPOL database and the cantonal police authorities have access to that index. This is permitted under current federal law. It is a matter for the **cantonal data protection authorities** to assess whether the verifications carried out by the **cantonal police** are lawful (Section 1.4.7).

### **Health**

Health insurers who process **SwissDRG**-invoices are required to set up so-called **data collection points**. These collection points must be covered by a **data protection certificate**. Thus for the **first time** in Switzerland, data protection certification has been made **mandatory** (Section 1.5.1).

Many of the ideas that were generated in the wake of the **eHealth projects** are reflected in the federal law on the **electronic medical record**. The FDPIC was involved in the work of the Federal Office for Public Health that was tasked with drafting the law. Many of his recommendations were taken on board (Section 1.5.2).



Since January 2012, the **Federal Law on Health Insurance** requires that all **insurance companies** that fall within its scope draw up **data processing regulations**. These must be presented to the FDPIC for evaluation and published. This provision incorporates and expands on Article 21 of the Data Protection Ordinance (Section1.5.4).

### **Insurance companies**

**Health insurance companies** must allow staff access to **insured persons' health records** for the settling of health insurance claims. Ideally, employees should only have access to the data that are required **for the specific claim**. Once the claim has been processed, authorization to access the data should be removed. However, there is a big gap between ideal and reality, as was clearly demonstrated after an **examination of the facts** in the case of a major health insurer (Section1.6.1).

### **Workplace issues**

On 12 April 2012, the **Federal Administrative Court** decided that in future **pension fund statements** are to be issued in such a way that **only the insured person** knows what the fund statement says. The information must not be accessible to third parties. The FDPIC has carried out a **verification** to ensure compliance with the court ruling (Section1.7.2).

A number of **banks** have transmitted documents to the **US authorities** containing the names, email addresses and telephone numbers of former and current bank **employees** and well as those of **other individuals**. The FDPC carried out a **case investigation** at 5 of the banks concerned and issued a series of **recommendations** which banks are asked to implement in order to ensure **greater transparency** (Section1.7.3).

IT technology has developed rapidly over the last few years and has **radically changed workplace practices**. **Employers** have an increasingly wide range of **technical monitoring and control systems** to choose from. This raises the issue of what kind of supervision is allowed and when do controls go too far (Section1.7.4).

What happens to **email accounts** in the event of an unexpected absence? To what extent is the **employer** entitled to consult the **emails of the employee** in question? These are just two of the most frequent questions that crop up when people contact the FDPIC's **telephone hotline**. The protection of personal integrity and privacy at the workplace must be covered by an appropriate **regulatory framework** (Section1.7.5).

### **Business and commerce**

At the request of one of the major retailers, the FDPIC was asked to look at the data protection implications of a **shopping basket analysis** carried out on the basis of data obtained from **customer cards**. Modifying the way data is processed, as in this case, requires compliance with **even higher standards** in terms of **transparency** and obtaining the **consent** of customers (Section1.8.1).

**Moneyhouse, the credit reference agency**, offers a contact search service. This involves the publication of **address data on the Internet** which the person in question may have **blocked**. The FDPIC has undertaken a fact-finding mission in order to take a closer look at the type of data processing involved (Section1.8.2).



Last summer, two cantons introduced a **new practice** which they are applying to their **commercial registers** as part of the implementation of the principle of public access to official records. Any person submitting a request for information will automatically receive **by email all the relevant documentation**. The switch from a consultation process involving a trip to the company register office, or at least a personal contact, to a form of generalised **access via the Internet** in line with the **principle of public access**, raises a number of serious issues with regard to data and privacy protection (Section 1.8.3).

The **commercial register** is to be modernized. The plan is to create a **centralized electronic database** which will be supported by a uniform software system. From a data protection perspective, the FDPIC welcomes the decision to make the commercial register system compliant with the **«right to be forgotten» principle** (Section 1.8.4).

The FDPIC has issued his opinion of the **revision of the Postal Ordinance** within the context of the interministerial consultations. In the light of the liberalization of the postal market, he clearly set out his position with regard to the duty to provide information and the **handling of address data**, in particular the **transmission** of such data **to third parties** (Section 1.8.6).

### Information and awareness-raising

One of the FDPIC's key tasks is to **inform and raise the level of awareness of the population** regarding data protection and the principle of transparency. Information about current issues is regularly published on his website [www.derbeauftragte.ch](http://www.derbeauftragte.ch). Last year, he explained the position of the data protection authorities on the subject of **naming and shaming activities on the Internet**; on the processing of data at **mass sporting events** or in **libraries**; and he co-published an updated and expanded booklet with the Federal Department of Justice on **Frequently Asked Questions about the Freedom of Information Act**. In order to mark the **Data Protection Day** on 28 January 2013, the FDPIC issued a brochure on data and privacy protection at the **workplace**. For **training purposes**, members of the FDPIC's staff gave a series of lectures to students at the University of Lausanne. Last but not least, the FDPIC participated in joint events organized with the data protection and information advisors of the Federal Administration and the cantonal mediation offices (Sections 3.1 to 3.5).

### Principle of transparency (freedom of information)

In 2012 the **federal authorities** received 506 more **requests for access to information** than the preceding year, representing an increase of 8%. Of the 258 cases where requests were either entirely or partially refused, 78 were submitted to the FDPIC for mediation. In the year under review, **61 requests for mediation** were **settled**, of which 41 were still pending from the two previous years.

There were once again **several court decisions** relating to the principle of transparency. Thus, the Federal Administrative Court was asked to rule whether the **compulsory fee**, which is established by the Freedom of Information Act, also applied to **media professionals**. The Court ruled that the Federal Council (Swiss government) had not availed itself of the opportunity of introducing a general fee exemption in the Ordinance on the implementation of the Freedom of Information Act. The judges held that granting a general exemption would in any case have been incompatible with the **principle of legal equality**. The Supreme Court has in the meantime overturned that decision. The country's highest



court ruled that the Freedom of Information Act imposed an obligation on the Federal Council to show consideration for the needs of the media.

Continuing on the subject of transparency, the FDPIC expressed his position on a number of political proposals. As mentioned last year, there have been a few isolated attempts to **remove** certain activities, and even entire government agencies, **from the scope of the Freedom of Information Act**. A draft Intelligence Service Act tried to do precisely that. The FDPIC rejected this recommendation because the Freedom of Information Act applies to the entire federal administration, and the law in any case provides sufficient exceptions to cover sensitive information. The Federal Council did not follow the FDPIC's arguments (section 2).

The full version of the annual report can be obtained on the Internet at [www.derbeauftrage.ch](http://www.derbeauftrage.ch) or a hard copy may be ordered from BBL, Vertrieb Publikationen, 3003 Bern: Art. No. 410.020

Copies may also be ordered via the Internet at:  
<http://www.bundespublikationen.admin.ch/de/publikationen/artikelsuche.html>