



Embargo : 25 June 2012 at 10 a.m.

25th June 2012

Summary of a selection of issues covered in the 19th Report on Activities

Transparency principle

In 2011 the number of requests for access to information held by the federal authorities almost **doubled** over the previous year, whereby the ratio between the number of requests granted and those denied remained more or less the same. There was also a twofold increase in the number of requests for mediation: in 254 cases where access to information was either denied or only partially granted, 65 were submitted to the FDPIC for mediation, corresponding to a proportion of approximately 26%.

Overall, **30 requests for mediation** were successfully handled over the past year. Of all the procedures involving either mediation or a recommendation, 85% of cases led to a more **favourable outcome** for the applicant compared with the original position of the authority to which the request for information had been submitted. As a result of the partial revision of the Ordinance implementing the Government Transparency Act, the time allowed for establishing a mediation procedure in cases which are particularly time-consuming has been extended.

Some authorities have been attempting to have certain of their activities **removed from the material scope of the Transparency Act**. It was against this background that the FDPIC took a position on the planned revision of the antitrust law. In his view, the Transparency Act does, under certain circumstances, provide **sufficient legal possibilities** to refuse, restrict or postpone access to public records. Moreover, the FDPIC has always recognized the fact that certain official documents need a higher level of protection. This explains why the FDPIC, in a report to the Federal Council, argued that the competition authorities should be fully subject to the Transparency Act. The Federal Council heeded his advice (Section 2).

Health

Two **case investigations involving the Swiss Accident Insurance Fund (SUVA)** have produced a positive outcome. On the one hand, SUVA took the necessary steps to ensure the systematic registration of files and can in principle therefore guarantee a **right of access to information in accordance with the Data Protection Act**. On the other hand, the inspection revealed that **case management** per se does **not raise any data protection issues**. Nevertheless, the FDPIC identified shortcomings in the management of access rights of insured persons. SUVA recognized the problem and took immediate measures to limit the number of persons authorized to access data (Sections 1.5.3 and 1.5.4).

Clinical studies where personal data are used not only for the treatment of patients but also for research purposes raise some **highly sensitive data protection issues**. The FDPIC has recommended that a suitable solution be found to ensure that the transition from treatment to research be clearly defined in the study design. At the point of transition, personal data must be **anonymized** (Section 1.5.7).



Insurance

The FDPIC has completed his examination of the «**car claims information pool**», an electronic data platform for motor vehicles. His recommendations for the improvement of data protection and data security were accepted (Section 1.6.2).

Workplace issues

The telephone helpline set up by the FDPIC received numerous calls relating to cases involving **workplace surveillance**. Clearly neither the employers nor employees really know what is **really permitted**. The employers are primarily concerned to ensure that their procedures comply with data protection requirements, whereas the employees, while they may have no objections of principle regarding workplace surveillance, want to know exactly what the employers are allowed to do (Section 1.7.1).

Internet

Mobile devices use **geographical positioning data** in order to provide **location-based services**. If such data are stored over a long period, they can be used to establish a detailed user **movement profile**. In a case investigation, the FDPIC analysed Apple's data processing system; at the same time, Apple has now launched a software update which can be used to suppress the capture of geographical positioning data (Section 1.3.1).

In November 2009, the European Parliament revised the **directive on the protection of privacy on the internet**. One of the major changes that was introduced involved rules on the storage of, and access to, information such as cookies on a user terminal. The opt-out clause under the old directive was replaced by a so-called **informed-consent solution**, according to which the user has to opt-in after being provided with detailed information about the type and purpose of the data processing (Section 1.3.2).

There is a **website** which is used by tenants to **comment on and evaluate their landlords**. The aim of those who operate this information and evaluation platform is to create more transparency on the rental market. However, platforms such as this can raise a number of **legal issues** from a data protection perspective (Section 1.3.6).

A **computer game** released in the autumn created quite a stir in the press. The copy protection attached to the game was designed to **spy on users' computers** and to transmit to the manufacturer **information** stored on the computers relating to user behaviour and much more besides. The FDPIC is currently checking to see whether this much criticized programme complies with data protection requirements (Section 1.3.8).

The operators of websites have access to the **addresses of all visitors** who fill out a contact form either to send a message or to request information. It is not surprising that they use these addresses to **send out a questionnaire for the purpose of evaluating the website**. However, as the address data are a form of personal data, such practices are not generally allowable (Section 1.3.9).

Whoever looks for **information on the website of the Federal authorities**, on particular areas of policy or health-related issues, for instance, has to be able to trust that **great care will be taken with any personal data involved**. Federal bodies need to take particular care to comply with data protection provisions (Section 1.3.10).

It is in the interests of the Federal Administration to monitor the **use of information and communication technologies**. This is necessary to ensure that systems operate in the proper manner and that abuse is prevented. In order to be able to carry out this monitoring in accordance with the law, the necessary legal basis has been established (Section 1.3.11).



Business, Economy, Finance

A question which comes up again and again is how far **telephone company employees should have access to customer data**. Some employees need access to such data in order to do their jobs. **Accessing that data for private purposes** does, however, constitute an abuse and must be prevented by taking the appropriate organizational and technical measures (Section 1.8.3).

According to the FDPIC, when a telephone subscriber has an **asterisk placed against his name in the telephone directory**, he is indicating that his personal data are not to be used for any advertising whatsoever, i.e. not only telemarketing, but also addressed mail. This is not the current interpretation applied by advertising professionals who collect all the addresses in the telephone directory that are marked with an asterisk and use them for customer acquisition purposes (Section 1.8.6).

The study published in 2011 by the Federal Department of Justice on **electronic standards applicable to debt enforcement and bankruptcy law (eSchKG)** addressed the modernisation of the debt collection system in Switzerland and highlighted the opportunities and risks associated with the establishment of a **virtual Swiss debt collection office** together with a central debt collection register. Such a register is dependent on the introduction or use of a personal identifier (Section 1.9.2).

Biometrics

In the light of the **court ruling in the KSS case**, according to which the **central storage of biometric data** relating to recreational activities was held to be **disproportionate**, the question arises as to how such data may be stored in such a way as to meet data protection requirements. The FDPIC has examined a number of different scenarios and has published the results on his website. The purpose of this exercise is to meet the **needs of system operators**, on the one hand, and the **privacy rights of the persons concerned** on the other (Section 1.2.7).

Miscellaneous

The **letter** sent by the **Federal Statistic Office**, requesting that citizens participate in surveys, now clearly mentions whether participation is voluntary or mandatory. This change was introduced at the request of the FDPIC. Progress has also been made in improving quality assurance on the part of the company carrying out the survey (Section 1.1.1).

Recently, an increasing number of citizens have been turning to us with questions **regarding statistical surveys**. Most of these concern the **proportionality** of the evaluation, the use of the AHV-number (social security number) and a duty to answer requests for information. The FDPIC continually focuses his attention on such activities (Section 1.1.2).

In October 2007, a member of parliament tabled a parliamentary motion instructing the Federal Council to examine the possibility of **facilitating data exchange between the Federal and cantonal authorities**. A broad-based survey has proven thereupon that **data protection requirements cannot be blamed for any shortcomings in these data exchanges** (Section 1.1.6).

Information and public awareness

The FDPIC uses various means to make people more aware of data protection matters and the principle of transparency. On his website www.derbeauftragte.ch, for example, he regularly publishes information on current issues. Last year, amongst other things, he published a commentary on cloud computing and on the revised EU e-privacy directive. He is also active-



ly involved in promoting the training of specific target groups, for example at the Universities of Neuchâtel and Lausanne. Within the context of the sixth data protection day, a course for young adults on data security was devised (Sections 3.3 to 3.6).

The full annual report can be downloaded from the Internet at the following address www.derbeauftragte.ch or can be ordered from BBL, Vertrieb Publikationen, 3003 Bern:

Art. No. 410.019

Orders via the Internet can be placed at the following address:

<http://www.bundespublikationen.admin.ch/de/publikationen/artikelsuche.html>