



Not to be published before 03.07.2006, 10.00h

03 July 2006

Summary of various issues covered in the 13th Annual Report

Justice, Police, Security

In his last report, the Swiss Data Protection Commissioner (SDPC) announced the modification of procedures governing the verification of indirect information rights in the light of a decision by the Federal Data Protection Commission (FPDC). At a meeting with the FPDC and the Federal Office of Police, the SDPC discussed the new practices as well as experiences, difficulties and positive aspects encountered in connection with **indirect information rights**. Following the meeting, the Data Protection Commission announced that it was now in a position to authorize the SDPC's new practices with regard to the examination of requests for indirect information (Section 3.1.3).

The Federal Office of Police (FOP) submitted to the SDPC a draft proposal regarding the JANUS information system to take into account the need to provide **data subjects with the possibility of gaining retrospective access to police-related information** as required by law. The FOP felt that there was no need to adopt a similar approach for the GEWA information system as it was not responsible for the collection of the original data. After analysis of the JANUS concept, the SDPC suggested certain modifications. He also requested that the FOP develop a similar concept for GEWA. The FOP did not consider it necessary to act on his recommendations and stuck to its position on GEWA. The SDPC submitted the matter to the Federal Department of Justice and Police for decision (Section 3.1.4).

The SDPC has given his opinion on two draft proposals relating to **money laundering**. His comments regarding the need for a clearer specification of the legal basis were not taken into account, and this divergence of views is mentioned in the Federal Council's recommendation (Section 3.2.1).

Health

The issue of data processing by **Spitex Services** (home care) begs the question as to whether federal or cantonal data protection law applies. The Federal Department of Justice comes to the conclusion that as a rule, such activities by Spitex should come under the supervision of the cantonal data protection authorities (Section 4.1.3).

Computers have become standard equipment in all doctors' surgeries, especially because all medical acts have to be invoiced electronically as of 2006. The planned introduction of a health insurance card will promote their use even further. Questions raised by the SDPC show that service providers are unsure how they can ensure the necessary access as well as the **protection of electronic medical records**. One solution might be to have a logical or physical separation of the data (Section 4.1.6).

Insurance

The SDPC has been increasingly confronted with cases where **social health insurance companies** have communicated patient data to cardiology centres. They have done so even though they are strictly bound by **legal confidentiality provisions**. If patients do not give written consent for such data to be transmitted, insurance companies can be held responsible for illegal infringement of personality rights. In such cases, data subjects are entitled to seek redress not only in the civil, but also in the criminal courts (Section 5.1.3).



One **third-party liability insurer** has come up with a plan allowing for the **collection of incident data**. The company has developed a data protection leaflet and an authorization clause. Although there is still room for improvement, the insurer has made a welcome effort to ensure that patient data is only obtained from the treating doctor with the patient's written consent (Section 5.2.1).

Data Protection and Data Security

All activities carried out on a computer leave traces, some of which may contain personal data. The collection and processing of such data are covered by the Data Protection Act. According to Swiss law, the Federal Administration may only process such data if there is a legal basis (Section 2.1.2).

Work-related Issues

The **admittance procedure into a pension fund** invariably involves the collection of health data. Unfortunately health questionnaires seem to become increasingly detailed and extensive. That is why it is very important that the applicant's medical data remain with the medical services. Communication of such data to the pension fund is deemed unreasonable and in any case is not allowable without the express consent of the person concerned (Section 6.2).

As far as work-related issues are concerned, **GPS** (Global Positioning System) **technology** allows the systematic tracking of all company vehicles and is used to check the productivity of sales reps and field workers. As far as personality rights and health protection are concerned, this measure does not raise too many concerns, provided that the principle of proportionality is respected (Section 6.3).

Trade and Commerce

The use of personal data for marketing activities targeted at one's own clients always raises a number of issues and often angers the persons concerned. Swisscom Fixnet has developed a form which allows its customers **to selectively choose the marketing channels through which they may be contacted** (Section 7.3).

Biometrics

Biometric access controls are being increasingly used in public buildings and facilities. In order to respond to the concerns of season or subscription ticket-holders, the SDPC decided to verify the biometric access control system of a private sports centre. He is currently in the process of analyzing the data to ensure that they comply with data protection principles (Section 2.2.5).

From December 2004 to the middle of April 2005, a pilot project named Secure Check was installed at Zurich airport. Secure Check is designed to speed up passenger security checks and passport control procedures before departure by means of biometric data and to shorten waiting times for airline travellers at checkpoints. Controlling the use of **biometrics at check-in and during boarding**, the SDPC comes to the conclusion that the handling of biometric personal data generally satisfies data protection requirements. However, the pilot project at Zurich airport did raise some basic concerns (Section 2.2.6).

Miscellaneous

Within the framework of the revision of the Data Protection Act, a voluntary **data protection certification procedure** has been put in place. Regarding the certification of organizations, it has been decided that certification companies would be provided with a two-part reference model. The first part deals with the criteria that must be fulfilled by a data protection management system, whereas the second part focuses on conformity verification procedures, i.e. the concrete data protection requirements that are derived from the Data Protection Act (Section 1.1.1).



On the subject of **naturalization procedures** by a decision of municipal-level assemblies or plebiscites, the publication of candidates' personal data for citizenship purposes is considered unreasonable from the point of view of the protection of the individual's privacy. One possible solution which complies with the Data Protection Act would involve allowing a limited number of persons, for instance a special commission, to have access to the candidate's file on condition of preserving confidentiality (Section 1.2.2).

The DDPS (Federal Department of Defence, Civil Protection and Sport) is seeking a **partial revision of the Swiss Military Act**. One of the primary aims is to create a clear and specific basis for the processing of personal data. The preliminary draft still needs to be improved so that it complies with data protection requirements (2.2.2).

Over the last few years, organizers of **major sports events** have increasingly taken to selling **personalized tickets**. Concurrent with this trend, the authorities have enacted legislation to combat violence and hooliganism at such mass sports events. The SDPC monitors the legislative process in the area of public security. At the same time, he has held discussions with those responsible for ticket sales for the EURO 2008 football championships, at least for the games that will take place on Swiss soil (Section 2.2.7).

For Swiss companies intending to have their data collection processed abroad under an **outsourcing** arrangement, the SDPC recommends the use of a contract to cover the cross-border disclosure of data. Together with David Rosenthal from the Homburger law office in Zurich, the SDPC has developed a standard contract (Section 1.2.3).

International Affairs

The various drafts of the 2nd generation Schengen Information System (SIS II) which have been discussed by committees and working groups at European level will have repercussions on the implementing regulations in Switzerland. The SDPC has presented his concerns on this subject within the context of the interdepartmental consultation process. He also participates in meetings of the group set up under the provisions of Article 29 of EU Directive 95/46/EC which considers the protection of individuals with regard to the processing of personal data as well as meetings of the joint supervisory body of the SIS (Section 9.1.1).

European Data Protection Commissioners attended a meeting in Krakow on 25 and 26 April 2005 upon the invitation of the Polish Inspector General for Personal Data Protection. The Data Protection Commissioners adopted a declaration in which they call for the adoption of a legal instrument for the processing of personal data within the context of police and judicial co-operation in the European Union. The European Data Protection Commissioners also held two further meetings, one on 16 September 2005 in Montreux, and the other on 24 January 2006 in Brussels. During the Brussels Conference, they adopted an opinion on the EU Council's Draft Framework Decision on Data Protection in the area of police and judicial co-operation (Section 9.1.2).

The 27th International Conference on Privacy and Personal Data Protection was held in Montreux from 14 – 16 September 2005. The meeting, which was organized by the SDPC, brought together data protection authorities from over 40 countries around the world. At the end, a declaration was adopted in order to confirm the universality of data protection principles. Furthermore, the data protection authorities adopted a resolution on the use of biometrics in passports, identity cards and travel documents, as well as a resolution on the use of personal data for political communication (Section 9.2.1).



New Publications from the SDPC

In December 2005, the SDPC published for the first time after a two year break **a new newsletter called *datum***. *datum* will appear twice a year and is intended for a broad public that is interested in data protection issues but does not necessarily have a high level of expertise (Section 10.2)

The full annual report can be accessed in German and French on the internet (www.edoeb.admin.ch) or may be ordered from BBL, Vertrieb Publikationen, 3003 Bern:
Art. Nr. 410.013

Order via the internet:
[http: //www.bbl.admin.ch/de/bundespublikationen/shop/zivil/index.htm](http://www.bbl.admin.ch/de/bundespublikationen/shop/zivil/index.htm)