



Embargo: 28 June 2010 at 10 a.m.

28 June 2010

Summary of the issues covered in the 17th Report on Activities

Health

There is a need to create a clear legal basis for the ordinance of the Federal Department of Home Affairs on **preventing the spread of new emerging infectious diseases**. This is particularly true in view of a lack of clear regulations regarding cross-border disclosure of personal data (section 1.5.1).

The FDPIC had to slightly adapt the **«explanatory note on patient discharge and surgery reports»**, as a Federal Court ruling has clarified the rights of insurance companies regarding such reports. In principle, however, the FDPIC adheres to a policy of progressive communication of information to the insurance company (section 1.5.5).

If a Swiss company sends a **blood sample to South Africa for laboratory analysis**, then a contract must be concluded to guarantee adequate data protection (section 1.5.6).

Insurance

Particularly sensitive personal data are handled as part of a **case management** process. As case managers work both in the interests of the client and those of the person concerned, conflicts of interest may arise. The principles of purpose limitation and transparency must therefore be scrupulously respected (section 1.6.1).

On examination of a pension entitlement, the insurer can also demand **inspection of records dating from the period before the granting of the pension**. In this case the principle of proportionality shall apply (section 1.6.3).

The **Federal Social Insurance Office** intends to provide cantonal compensation funds and disability insurance offices with access to the **eRegress** database so that they can process appeals relating to old age and survivors' insurance and disability insurance electronically. Although the FDPIC understands the need to make this data available using **data retrieval procedures**, it was unable to give the green light to the plan as the principle of legality applies to federal bodies. The necessary legal bases are clearly not present in the applicable social security legislation. In order to create a federal database, an adequate formal legal basis must be created (section 1.6.5).

A political party has published a telephone number which allows citizens to report **alleged abuse of the welfare system**. This gave rise to various legal issues. The FDPIC maintained that although combating abuse of the welfare system is in the public interest, it is **exclusively the task of the competent authorities** to handle such information (section 1.6.6).

The work environment

Swiss Post presented a **health management project** to the FDPIC, the aims of which are **preventative healthcare, absence management** and illness and injury **case management**. This involves the treatment of employee health data by the employer. The FDPIC has analysed the project and has no objections providing certain conditions relating to data protection are fulfilled (section 1.7.5).

As a result of media reports, the FDPIC took a closer look at the **Lidl** retail company, and more specifically its **video surveillance** and **workplace search practices**. It was found that employees were not



being given sufficient information, but that the handling of employee data was in conformity with data protection provisions (section 1.7.6).

The market for credit and commercial information is a highly competitive one which forces companies to constantly innovate. Thus a credit agency sought to sell personnel managers **data on the credit-worthiness** of new or existing **employees**. The Federal Administrative Court accepted the request of the FDPIC for **preventative measures** with regards to this service (section 1.7.7).

Trade and Industry

Company mergers are the order of the day in the business world. These also involve working with personal data and there are particular risks of unauthorised individuals gaining access to personal information, of too much data being communicated (either too soon or to the wrong people), or of personal data being misused. The FDPIC has defined these risks and recommends **measures** to avoid any violations of privacy (section 1.8.2).

The revision of the Data Protection Act, in force since 2008, allows for company self-regulation. Providing companies appoint a **data protection officer** and inform the FDPIC, they no longer have to register their data files. However, the hierarchical position and the professional qualifications of the officer must fulfil certain **criteria**. The FDPIC has set out these requirements in his explanatory notes (section 1.8.3).

Following his recommendation of December 2008 on the tenant screening service «**Mieter Check**», the FDPIC held in-depth discussions with the company **Deltavista AG** on implementation procedures. During the follow-up inspection carried out in autumn 2009, the company presented a system and handed over documents which the FDPIC regarded, in the form presented, as adequate from a data protection point of view and in accordance with his recommendations. Consequently the supervisory process to verify compliance is now concluded (section 1.8.5).

Finances

Following the conflict relating to US access to **financial transaction data** stored on the servers of SWIFT, the financial service provider, the latter has now opened two new data processing centres in Switzerland. This is a move to meet the concerns of the European data protection authorities and the FDPIC. Furthermore, the USA is currently in negotiations with the EU on an agreement to facilitate access to SWIFT data stored in the EU as part of the fight against international terrorism (section 1.9.1).

A start-up company has approached the FDPIC with various data protection issues relating to **cross-border factoring**. From a data protection point of view, a basic distinction needs to be made in this case between assignment of debt and debt collection, as different provisions apply in each case (section 1.9.3).

The **ordinance on the new VAT law** provides for a computerised data access procedure. In the field of tax legislation both the principles of legality and tax secrecy apply. Our comment on the data access procedure and our proposal for a separate data protection ordinance were completely ignored in the draft ordinance on the VAT law. The data access procedure thus lacks an adequate legal basis (section 1.9.4).



Internet

The **new old age and survivors insurance number** is increasingly being used in different eGovernment projects as a **personal identification number**. There is a tendency to forget, however, that the use of this number for such purposes has to be regulated by law (section 1.3.1).

People nowadays are **mobile**. They want to be able to work **anywhere** and have **access to documents** wherever they are: at home, in the office or on the go. Possible solutions to this dilemma are storing the data on a portable data storage device or on the internet. Each solution is associated with different risks, and suitable measures are available to counter such risks. The FDPIC has examined them in detail. He has also scrutinized **the data protection aspects of internet search engines**, as these collect targeted information on the search strategies of those surfing the internet as well as the quality of the results, and subsequently carry out a statistical evaluation of the information gleaned (section 1.3.6 and 1.3.7).

Miscellaneous

The **Swiss Accreditation Service (SAS)** has accredited the first private companies for data protection certification of their organisation and procedures. The FDPIC supported the SAS in this task. The names of the accredited companies are published on the website of the SAS (section 1.1.1).

Thanks to the harmonisation of registers, the **census** will, for the first time in 2010, be carried out on the basis of the new system. Every year, as part of the census, large quantities of data will now be collected from citizens and processed. The FDPIC has supported several projects and noted that those involved are aware of data protection issues as a matter of principle (section 1.1.3).

The draft law on **research on human subjects** was passed in October 2009 by the Federal Council and referred to parliament for discussion. Prior to that, the FDPIC was able to give his views during interdepartmental discussions. The draft law provides an **escape clause** for researchers in the field of the re-use of biological samples and health-related personal data. FDPIC considers this escape clause to be highly problematic (section 1.1.5).

During the various consultation procedures on the **federal law on corporate identification numbers (CID)**, the FDPIC pointed out the supervision and privacy violation possibilities linked to the use of such a number in a B2B environment. He suggested banning, or at least restricting, the use of corporate identification numbers in this field. Furthermore the Federal Office of Statistics should only publish the CID on the internet with the consent of the person concerned (section 1.1.6).

The FDPIC has issued an opinion on the planned **traffic accident register**, consisting of a data collection register and an analysis register. As particularly sensitive personal data will also be handled, the data processing must be set out in a formal law (section 1.2.5).

As part of the complete revision of the **federal law on the promotion of gymnastics and sport**, the FDPIC has suggested two legal bases for doping controls and the facilitation of data exchange between the various anti-doping bodies. These suggestions were accepted and integrated into the law. The revised law improves legal certainty for sportsmen and women in the **fight against doping** (section 1.2.7).

Compliance with the Data Protection Act is also necessary in the case of **cross-border administrative assistance**. It should first be established whether administrative assistance is regulated by a special law. The issue is then to ensure that the privacy of the individuals concerned is not seriously jeopardised by data being communicated within another country, particularly because of a lack of legislation which would provide adequate protection. In this case, satisfactory guarantees must be provided. These can be established on the basis of a data protection clause in an agreement or, if necessary, in a declaration (section 1.2.10).



Encryption procedures are suitable precautions for protecting sensitive data on storage systems such as **hard discs** or **USB sticks**. It should be borne in mind, however, that operating systems or applications also place sensitive data in other files such as swap and temporary files which should also be protected. Encrypted data is normally accessed using a password, which should be as secure as possible. There are now several encryption tools available on the market. The FDPIC has tested the programs Rohos Mini Drive and TrueCrypt for their suitability (section 1.2.12).

New FDPIC publications

The FDPIC website serves as a platform with information about activities in the fields of data protection and the principle of public access to documents. Once again, last year, new texts and observations on various subjects were published. Publications included explanatory notes on corporate data protection officers, mobile data processing and corporate mergers, as well as information and tips on data protection risks young people face on the internet. The FDPIC also developed **training material** for young people and teachers as well as federal employees (section 3.3).

The full version of the annual report can be obtained in German or French on the Internet at www.derbeauftragte.ch or a hard copy may be ordered from BBL, Vertrieb Publikationen, 3003 Bern: Art. No. 410.017.

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