

**Annual Activity Report 2005/2006**  
**of the Federal Commissioner for Data Protection and Freedom of Information**  
**(Exerpt)**

**Annual Report for 2005 and 2006 of the Federal Commissioner for Data Protection and  
Freedom of Information**

**– 21st Annual Report –**

**C o n t e n t s**

<b>1 INTRODUCTION</b>	<b>4</b>
<b>2 THE LEGAL FRAMEWORK FOR DATA PROTECTION</b>	<b>5</b>
<b>2.1 Further development of data protection law</b>	<b>5</b>
<b>2.2 Structure of data protection supervision under scrutiny</b>	<b>7</b>
<b>2.3 The Act on Relief for Small Businesses is at odds with data protection requirements</b>	<b>10</b>
<b>2.4 Data protection audit – urgent need for regulation</b>	<b>11</b>
<b>2.5 Outsourcing in the administrative sector – another problem area for data protection</b>	<b>13</b>
<b>3 EUROPE AND INTERNATIONAL AFFAIRS</b>	<b>14</b>
3.2.2 The Prüm Treaty	14
3.2.3 Europol	16
3.2.4 Schengen	16
3.3.1 Whistleblowing – How to deal with tip-offs from insiders	19
<b>3.4 European and international cooperation in criminal matters</b>	<b>24</b>
<b>4 TECHNOLOGICAL DATA PROTECTION</b>	<b>25</b>
<b>4.1 The electronic health card: Continuing waiting</b>	<b>25</b>
<b>4.2 Video surveillance</b>	<b>28</b>
4.2.1 Video surveillance needs safeguarding, too!	29
4.2.2 Video surveillance at railway stations	30
4.2.3 Video systems pinpoint shortcomings by the body politic, too!	31
<b>4.3 RFID (Radio Frequency Identification)</b>	<b>31</b>
<b>4.5 Biometrics and data protection</b>	<b>34</b>
4.5.1 Technology	35
4.5.3 The electronic passport and the new identity card	36
<b>6 THE LEGAL SYSTEM</b>	<b>39</b>
<b>6.1 Line tapping pursuant to Sections 100a et seq. of the Federal Code of Criminal Procedure</b>	<b>39</b>

<b>6.3 Genome analysis in connection with criminal proceedings</b>	<b>43</b>
<b>6.5 Improved enforcement of intellectual property rights – Implementation of the IPR Enforcement Directive</b>	<b>46</b>
<b>6.6 Digital rights management</b>	<b>48</b>
<b>7 INTERNAL ADMINISTRATION</b>	<b>50</b>
<b>7.1 The law concerning aliens</b>	<b>50</b>
7.1.1 Draft act on the implementation of residence- and asylum-related directives of the European Union	50
<b>7.5 2011 Census – The countdown has begun</b>	<b>51</b>
<b>8 FINANCIAL MATTERS</b>	<b>52</b>
<b>8.2 Retrieval of account data by tax offices and other authorities</b>	<b>52</b>
<b>9 BUSINESS</b>	<b>56</b>
<b>9.1 The need to prevent profiling</b>	<b>56</b>
<b>9.4 SWIFT – Inadmissible transfer of data to US authorities</b>	<b>60</b>
<b>9.5 Warning and information system of the insurance industry – Uniwagnis</b>	<b>62</b>
<b>9.6 Federal Constitutional Court stops insurance companies obtaining consent by way of declarations on standard forms</b>	<b>64</b>
<b>10 TELECOMMUNICATIONS AND TELESERVICES</b>	<b>66</b>
<b>10.1 An error of judgement in Brussels – The directive on the retention of telecommunications data</b>	<b>66</b>
<b>12 TRANSPORT</b>	<b>68</b>
<b>12.1 Lorry toll</b>	<b>69</b>
<b>12.2 eCall</b>	<b>73</b>
<b>12.3 Event data recorder – Big Brother on-board?</b>	<b>75</b>
<b>12.4 Pay as You Drive – Know where You Go</b>	<b>76</b>
<b>15 DEUTSCHER BUNDESTAG – FEDERAL PARLIAMENT</b>	<b>77</b>
<b>15.1 Online facility “Public petitions”</b>	<b>77</b>

## 1 Introduction

Information technology has changed dramatically since the Federal Constitutional Court's 1983 "census judgement" established data protection as a fundamental right. The integration of computer chips into all types of everyday items has led to a recording of our behaviour, our interests and our personal characteristics and increasingly lays them open to monitoring and surveillance. While 25 years ago the prospect of every aspect of our lives coming under surveillance was rendered unlikely by a lack of processing capacities and high costs, the limiting effect of these factors is now drastically diminished. This underlying trend has played a particularly predominant role in shaping the period under review in this report. Politics, business and science communities are thus called upon to adopt a responsible approach to the available technology and to impose restrictions on their own activities. The apparent expediency of a measure does not necessarily justify its actual application. The effects on the individual right to self-determination must always be considered in decisions on the use of IT systems.

In view of these underlying developments, substantial efforts might be expected on the part of the legislature with an aim to countering these risks. Regrettably, there is little sign of any such initiative. Instead, the response to the possible abuse of information technology comes in the form of more and more control measures which for the most part affect innocent parties. In the attendant political debate the Internet is sometimes referred to as a "school of terrorism", for example, in order to justify the most comprehensive surveillance possible. The fact that criminals also make telephone calls or send e-mails was the starting point for the decision adopted at European level at the beginning of 2006 to require providers of electronic services to store all traffic data of all users for six months, irrespective of any concrete suspicion or reasons. This line of logic ultimately led to calls for prosecuting authorities and intelligence services to be able to secretly access computers via the Internet in future. The finding by the Federal Constitutional Court that such "online searches" are without legal foundation does not lead representatives of the security authorities to consider whether such measures encroach to an unreasonable extent on the right to determine the use of one's personal data. Rather, it gives rise to calls for this investigative method to be legitimised in law.

The advance of the information society is irreversible. Influence can be brought to bear, however, to decide whether this society is to offer the individual greater opportunity for development or whether it is to be characterised by ever more extensive control and surveillance. In this context it will be of central importance how the legislature makes use of its capacity to shape the future course of development – by strengthening fundamental rights or by legitimising ever more restrictions on fundamental rights. Against this background I consider it disturbing that numerous restrictions on data protection have become law in the period under review, leaving the Federal Constitutional Court to rescind disproportionate encroachments on fundamental rights.

The right to determine the use of one's personal data is one of the most important civil rights in the information society. Effective control of the technology-related risks in the area of monitoring and surveillance is not to be expected without statutory restrictions. This applies not only to the relationship between the state and its citizens, but also to the handling of personal data by the business community. The indication by the Federal Constitutional Court

that comprehensive personal profiles are not reconcilable with the concept of humanity embodied in the Basic Law is more pertinent than ever, in the face of increasingly effective means of collecting, collating and evaluating data. This makes it all the more alarming that the much heralded adaptation of data protection law to new technological developments has made no progress whatsoever to date, while there is no lack of legislative projects to restrict the right to determine the use of one's personal data. In view of this disturbing imbalance it is worth remembering that the principles of human dignity and proportionality which are enshrined in the Constitution are of crucial importance to a democratic information society. This means that there is no place for all-encroaching surveillance or monitoring measures which invade the individual's most private sphere.

Notwithstanding the fact that this report is presented in the first person, it should be noted that the relevant activities were carried out for the most part by my staff. My thanks go to these staff members for their great commitment and successful work. Our capacities are now strained to the limit, however. The number of petitions alone has almost doubled in recent years. The additional post of Federal Commissioner for Freedom of Information has been introduced, without new staff being provided in the number stated on the preface sheet to the bill. Unless our staff is bolstered accordingly, it is thus foreseeable that we will be unable to continue our work at the present level of intensity and standard of quality.

I also wish to thank the delegates of all parliamentary groups of the German Bundestag who have taken a sustained interest in data protection and demonstrated a corresponding level of commitment, and the representatives of public and private agencies for whom data protection is a key factor in successful operations.

Peter Schaar

## **2 The legal framework for data protection**

### **2.1 Further development of data protection law**

*The urgently necessary modernisation of data protection law has yet to materialize.*

The fundamental reform of data protection law, which has been heralded for many years now and repeatedly urged by the German Bundestag (cf. 20th Annual Report, no. 2.1; 19th Annual Report, no. 3.3) has once again failed to materialise in the period under review, although considerable potential exists here for modernisation of the administrative system, debureaucratization and a strengthening of civil and consumer rights. A new concept of data protection whereby the present system based on prohibition, monitoring and the imposition of sanctions would be complemented or even replaced in certain areas by an integrated approach, regarding data protection not as a restriction but as a competitive advantage and a source of added value, could make an important contribution towards modernising the state and society. This would involve the integration of data protection into technical systems and methods from the outset, self-regulation and self-monitoring in the field of data protection and a strengthening of the possibilities for protection available to data subjects themselves.

In the absence of appropriate reform measures, the discrepancy between technological advances and the use of electronic data processing in ever more areas of life on the one hand and the applicable provisions of data protection law and the system of controls in the field of data protection law on the other is growing ever wider. I have thus repeatedly pointed out that there is an urgent need for the ongoing development of data protection law and its adaptation

to the quickly changing underlying conditions. Once developments are allowed to head off in the wrong direction, redressing mistakes becomes a difficult matter requiring a considerable scope of legislative action.

At the beginning of the current legislative period, the Conference of the Commissioners for Data Protection of the Federation and the Länder thus appealed to the parliamentary groups in the German Bundestag and to the Federal Government to step up their support for protection of the fundamental right to determine the use of one's personal data, stating the most important areas in which action is required (cf. box on no. 2.1).

The following should be considered as initial reform measures:

- A simplification of current data protection law. In addition to the Federal Data Protection Act, a plethora of special rules and regulations of varying scope also applies in this area at present, resulting in a generally confusing picture for all parties involved. Simplifying and harmonizing this field of legislation would represent an important contribution towards debureaucratization.
- The establishment of a standard nationwide data protection audit pursuant to Section 9a of the Federal Data Protection Act (see no. 2.4) as a starting point for integrated data protection spanning all relevant systems and procedures.
- Improved protection and a strengthening of the rights of affected citizens to counter the ever more comprehensive collections of data in the private domain and the networking and evaluation of such data to the detriment of the data subjects (cf. no. 9.1).

I hope that initial steps will finally be undertaken for the urgently required modernisation of data protection law.

Box on no. 2.1

Extracts from the resolution of the 70th Data Protection Conference of 27/28 October 2005

**“Appeal by the Commissioners for Data Protection of the Federation and the Länder:  
A modern information society needs more data protection**

The Conference of Commissioners for Data Protection of the Federation and the Länder see a major need for action in the field of data protection in the 16th legislative period of the German Bundestag. The path towards a free and democratic information society deploying state-of-the-art technology compels all those involved to devote particular attention to the protection of the right to determine the use of one's personal data. Without more effective data protection, the advances above all in the areas of information technology and biotechnology will fail to gain the social acceptance which is necessary both for the business sector and for the administrative authorities.

A fundamental modernisation of data protection law is required. This must entail broadening the current data protection law based on monitoring and counselling to include instruments in

the areas of economic incentives, self-data protection and technical prevention. It is thus high time for a data protection audit act to be drawn up by the German Bundestag in this legislative period. The design of technology in compliance with the requirements of data protection as a means of stimulating competition is in the interests of the business community, the administrative authorities and the general public. At the same time, the faltering comprehensive amendment of the Federal Data Protection Act requires to be moved forward with vigour. A simplification and concentration of the statutory provisions will serve to reduce bureaucracy while strengthening the protection to fundamental rights.

The monitoring of data protection has failed to keep pace with the quite phenomenal advances in information technology. In some Länder, data protection monitoring continues to be carried out by subordinate bodies. The available manpower and technical resources are generally inadequate. This situation prevails despite the requirement under European law to carry out data protection supervision in complete independence and to provide adequate human and technical resources to this end.

The Commissioners for Data Protection of the Federation and the stated Länder appeal to the parliamentary groups in the Bundestag and to the future Federal Government to step up their efforts to protect fundamental rights in the information society.”

## **2.2 Structure of data protection supervision under scrutiny**

*The European Commission considers the data protection supervisory authorities in Germany to be insufficiently independent and has started an infringement procedure in this connection. The complex structure of the data protection supervisory system can also lead to other problems.*

The structure of data protection supervision in the Federal Republic of Germany is highly complex (cf. 20th Annual Report, no. 2.3) and often unclear to the general public. First and foremost, however, a fundamental condition pertaining to supervisory activities is that they must be conducted free of any influence by the state.

## **Infringement procedure of the European Commission**

Article 28 (1) of directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (official EC journal no. L 281 of 23 November 1995, p. 2 ff.) stipulates not only that one or more public bodies in the Member States must be charged with monitoring application of the national provisions adopted to implement the directive in their territory, but also that these bodies must discharge their allocated tasks in complete independence.

In response to a complaint submitted by a citizen, the European Commission examined whether this condition is met in the Federal Republic of Germany. It came to the conclusion that the manner in which the supervision of data protection is carried out in the non-public sector by the interior ministries of the Länder themselves or by authorities of the general Land administration is not in accordance with the requirements of the directive. The Commission observed that the same applied to the provisions whereby the task of monitoring compliance with data protection regulations is assigned to the data protection commissioners of the respective Länder but such monitoring is subject to supervision by the executive branch of the government with regard to technical aspects and points of law. The European Commission thus started an infringement procedure on 5 July 2005. Sharing the legal opinion of the European Commission, I subsequently approached the Federal Minister of the Interior and proposed a fundamental reform of data protection supervision in Germany, arguing that this would make an important contribution towards simplifying administrative procedures and cutting costs and would constitute an important step in the direction of a modern information society. In my statement before the committee for internal affairs and sport of the Land parliament of Lower Saxony I once again provided a detailed account of the legal aspects pertaining to the issue of the “complete independence” of the supervisory authorities for the non-public sector. In a resolution on the infringement procedure adopted by the Conference of Commissioners for Data Protection of the Federation and the Länder at its meeting in October 2005 (cf. box on no. 2.2), the Conference supports the legal opinion of the Commission and calls for corresponding changes to the supervisory structure.

The Federal Government adhered to its legal viewpoint that German law was in compliance with the requirements of European law. Discussions with the Commission failed to produce any results on this issue, prompting the Commission to submit a substantiated opinion on 15 December 2006 in accordance with Art 226 (1) of the Treaty Establishing the European Community, in which it establishes an infringement of Article 28 (1), sentence 2 of the directive and requires the Federal Republic of Germany to undertake the necessary measures to comply with the Commission’s view within two months. It is to be expected that the Commission will bring an action before the European Court of Justice after expiry of this deadline.

## **Consequences of the current supervisory structure**

Notwithstanding the important matter of the complete independence of the supervisory authorities for the non-public sector, which forms the subject matter of the treaty violation proceedings, the highly complex structure of the supervisory system in Germany (cf. 20th Annual Report, no. 2.3) gives rise to further difficulties. The large number of different and mutually independent supervisory authorities means that the same facts and legal aspects of a case may be judged and evaluated differently, which can be problematic in individual cases for companies and service providers operating nationwide in the private sector, as well as in



the public sector, e.g. for the security authorities. In order to counter these difficulties, the Conference of Commissioners for Data Protection of the Federation and the Länder for the public sector and the so-called “Düsseldorf Circle” for the non-public sector are endeavouring to share information and to coordinate their activities with an aim to achieving the most uniform possible interpretation of the law and procedures. This approach is very time-consuming and work-intensive, however, and owing to the independence of the respective supervisory authorities it can only result in harmonization, not in binding decisions. If a group of companies operating nationwide or an industrial federation wishes to obtain binding clarification of a data protection issue with the data protection supervisory authorities, for example, it may take many months for the Düsseldorf Circle to reach a final opinion, whereby this opinion will ultimately have no binding effect on anyone and will thus fail to offer the companies the legal certainty which they seek. This matter is also a frequent subject of complaints from the business community.

Undertaking a fundamental reform of data protection supervision could thus represent an important contribution towards the modernisation of administrative procedures and debureaucratization.

Box on section 2.2

**Resolution by the 70th Conference of Commissioners for Data Protection  
of the Federation and the Länder  
on 27/28 October 2005 in the Hanseatic City of Lübeck**

**Call for independent data protection monitoring in Germany**

In connection with an infringement procedure instituted against the Federal Republic of Germany by the European Commission on 5 July 2005 on the subject of the independence of data protection monitoring, the Conference once again calls for fully independent data protection monitoring.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EC data protection directive) requires compliance with data protection regulations to be monitored in the Member States by bodies which fulfil the tasks allocated to them in complete independence. In Germany, data protection monitoring for the private sector is now largely integrated in the chain of authority within the internal administration of the respective Länder. In the view of the European Commission, this supervisory structure for data protection monitoring in the private sector violates European law.

The Commissioners for Data Protection of the Federation and the Länder can ensure uniform data protection monitoring of the public and private sector on a fully independent basis. To this end, they should be established in all Länder and within the Federation as independent supreme authorities which are not subject to instructions from any other administrative bodies.

In this context, the intention in Lower Saxony to reallocate responsibility for data protection monitoring of the private sector from the Land Data Protection Commissioner to the ministry of the interior is a step in the wrong direction. The Conference is firmly opposed to this plan and calls on the Federation and all Länder to establish supervisory structures which conform with European law in the field of German data protection.

## 2.3 The Act on Relief for Small Businesses is at odds with data protection requirements

*The Act on Relief for Small Businesses eases the obligation to appoint in-house data protection officials for broad areas of the trade, handicrafts and professional sectors, thereby breaching European law.*

The Federal Data Protection Act has been amended in several provisions in Article 1 of the “First act to remove bureaucratic obstacles, particularly in the small and medium-sized business sector” of 22 August 2006 (Act on Relief for Small Businesses, Federal Law Gazette I, p. 1970). The provisions contained in the Federal Data Protection Act and in Section 203 of the German Criminal Code which facilitate the appointment of external data protection officials in particular for persons who are sworn to professional secrecy are to be welcomed without qualification, not least of all because they entail an affirmation of the fact that the Federal Data Protection Act also applies to lawyers, doctors and other professions which are subject to professional confidentiality.

I am particularly critical of the provisions which restrict the obligation to appoint data protection officials at business enterprises. The adopted amendments in Sections 4d and 4f para. 1 of the Federal Data Protection Act waive the obligation to register automated processing procedures and to appoint an in-house data protection official for enterprises at which a maximum of ten persons are deployed to carry out the automatic processing of personal data. As over 90 per cent of German companies have a workforce of under ten according to the Federal Statistical Office, the amendment to the Act has exempted broad sections of the trade, handicrafts and professional sectors from the registration obligation, without an in-house data protection official monitoring compliance with data protection requirements instead of such registration.

In my view, the law as it now stands is also at variance with European law, specifically Art. 18 (1) of directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (official journal L 281 of 23 November 1995, p. 31). The registration obligation is mandatory under European data protection law, without qualification and without any provisos as to the number of persons involved in handling data. In accordance with Art. 18 (2) of the directive, exemptions are only possible when an in-house data protection official is appointed or when, for categories of processing operations which are unlikely, with due regard to the data to be processed, to adversely affect the rights and freedoms of data subjects, the purposes of the processing, the data or categories of data undergoing processing, the categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the duration of storage of the data are stipulated in law. These conditions are not met in German law. In the context of European law, I thus consider it imperative that notification of the supervisory authorities or the appointment of an in-house data protection official be made compulsory.

It is questionable whether Section 4d para. 3 of the Federal Data Protection Act even met the requirements of European law in its previous version. Broadening the scope of this exemption is certainly no longer in compliance with the data protection directive. In November 2006, the European Commission thus voiced its reservations towards the Federal Republic of Germany

and requested a statement, also on the question as to whether and in what manner the data protection supervisory authorities in Germany have been consulted regarding these changes.

Contrary to the Joint Rules of Procedure of the Federal Government, there has been no such involvement on the part of my department, although far-reaching changes to data protection law have been undertaken. This is all the more regrettable as it has deprived me of any opportunity to propose and discuss alternatives which would have eased the workload for companies and self-employed persons with only a small number of employees while upholding the principle of in-house data protection monitoring. In this connection, it would have been worth contemplating not only the possibility of broadening the scope for appointing external data protection officials and further consolidating the legal basis for such appointments. Beyond this, it would also be appropriate to consider whether in-house data protection officials could be available at professional organizations and associations, such as craft guilds, chambers and trade organisations, to carry out competent and well-aimed internal data protection consultancy and monitoring for their members on request from the latter.

The amendment of the Act amounts to a de facto reduction of data protection in the relevant area. According to the letter of the law, it is true that only the obligation to register data processing procedures and to appoint in-house data processing officials has been revoked, while the statutory data protection requirements continue to apply. However, the controller is now required to ascertain himself what the remit of the in-house data protection official was under the Act, as is expressly stipulated in Section 4f para. 2a of the Federal Data Protection Act, which was newly inserted into the Act in the course of the parliamentary debate. This will serve to increase rather than to reduce the controller's workload, however. It is thus to be expected that the amendment of the Act will be misunderstood to amount to a reduction of data protection requirements for the affected small and very small businesses, as external monitoring by the supervisory authorities will generally be unable to identify and penalize any deficits in this area.

At the same time, the application of modern technologies, e.g. in electronic payment transactions, in the use of customer cards and, in the future, in the use of health cards and electronic ID cards, will hinge on the users' confidence that such technology is designed in conformity with the requirements of data protection and that data protection law is duly complied with at the bodies concerned. Against the background of the introduction and expansion of new technologies, a reduction in the scope of internal data protection monitoring could thus prove counter-productive.

## **2.4 Data protection audit – urgent need for regulation**

*Audit act fails to make any headway – an opportunity for modern data protection continues to be squandered.*

The German Bundestag resolved that a nationwide data protection audit should be introduced back in 2001, duly incorporating the corresponding Section 9a into the amended version of the Federal Data Protection Act of 18 May 2001 (Federal Law Gazette I, p. 904; cf. 19th Annual Report, no. 3.2.1). The appurtenant details, i.e. the specific requirements pertaining to examination and evaluation, the procedure and selection and approval of the appraisers are to be stipulated in a separate act (Section 9a, sentence 2 of the Federal Data Protection Act), however. Such an act has yet to materialize.

I have already reported several times on the importance of such an audit to modern, future-oriented data protection and the danger of the current standstill undermining this important initiative (19th Annual Report, no. 3.2.1; 20th Annual Report, no. 2.2). Although the German Bundestag resolved by a large majority to call on the Federal Government to submit an implementing statute on Section 9a of the Federal Data Protection Act in the current legislative period in response to my 19th Annual Report of 17 February 2005 (Bundestag document 15/4597; cf. box on no. 2.4), not even a ministerial draft bill or a benchmark paper for a possible regulation has been drawn up to date. Similarly, an initiative from the parliamentary sphere on which I reported in my 20th Annual Report (*loc. cit.*) has evidently not been followed up.

These years of hesitance in implementing a procedure which has essentially already been adopted by parliament remain incomprehensible. Administrative modernisation, increased efficiency and debureaucratization are guiding principles of political and legislative activity today. The data protection audit would fit seamlessly into such concepts, integrating data protection into procedures and products right from the concept development stage and providing economic incentives for data protection-friendly behaviour. As such, it could become an important element of self-regulation and effective consumer protection, without requiring any new bureaucratic measures by the state. There are already numerous models and criteria for the requirements to be applied to an audit, for the contract-awarding procedure and for the selection and appointment of appraisers which could serve as a basis for the swift and efficient establishment of an unbureaucratic data protection audit. There is also great demand for such an audit in the business community, particularly in the areas of IT and the Internet. This is confirmed by experience at Land level, where such an audit already exists for use in the Land administrations. I also frequently receive inquiries from the business community as to when a data protection audit in accordance with Section 9a of the Federal Data Protection Act is finally to be expected.

What is lacking, therefore, is not the need for such an audit, nor ideas and potential solutions for its implementation, but solely the necessary willingness on the part of the Federal Government to take this step towards modernizing data protection.

Box on section 2.4

Extract from the resolution of the German Bundestag on the 19th Annual Report of 17 February 2005, Bundestag document 15/4597:

2. The German Bundestag expects the Federal Government to submit an implementing statute on Section 9a of the Federal Data Protection Act in the course of this legislative period, in order to put an end to the sidelining of this important element of the latest amendment. The most unbureaucratic solution possible which is in line with the real interests of service providers and consumers is to be preferred here (19th Annual Report, no. 3.2.1).

## 2.5 Outsourcing in the administrative sector – another problem area for data protection

*The various agencies within the federal administration no longer discharge all their duties themselves. There is an increasing trend towards pooling cross-departmental tasks, inter-agency cooperation, joint e-government projects and the outsourcing of specific tasks to private companies. When personal data are involved, this becomes problematic from the point of view of data protection. Section 11 of the Federal Data Protection Act does not always provide an appropriate regulatory basis here.*

Pressure of costs, the streamlining of procedures, increased efficiency and the use of modern technology are prompting ever increasing numbers of administrative authorities to outsource some of the activities which they previously carried out themselves to other public bodies or private service providers, which is often paraphrased with the dazzled term “outsourcing”. In the federal administration, for example, private call centres are already being employed, post offices “privatized” and e-mail traffic with citizens handled through private service providers, without this being apparent to the outside world. When this involves the collection and processing of personal data, such practices are also of relevance to data protection issues.

Cases in which certain duties are transferred from one authority to another by law or within the organizational power of the Federal Government or the individual government departments, e.g. to concentrate the processing of similar matters at a single body, are generally unproblematic. As a fundamental principle, the permissibility of data processing is contingent on its being necessary in discharging the duty concerned. When the responsibility for discharging a duty is transferred, the previous body loses its authorisation to carry out the relevant data processing and the new body acquires such authorisation on assuming responsibility for the duty. Where necessary for the purposes of discharging the task concerned, the appurtenant data records at the previous body are to be transferred to the new body in accordance with the relevant regulations and deleted at the previous body.

The matter becomes more problematic when a transfer of duties between public bodies is not based on any corresponding organisational acts or when private service providers assume certain duties on a contractual basis. Section 11 of the Federal Data Protection Act is generally cited here and the process is specified as commissioned data processing, which means that no transfer of personal data of relevance to data protection is involved and the appurtenant legal requirements thus do not need to be observed. This is stretching Section 11 of the Federal Data Protection Act well beyond its actual regulatory scope. According to its wording, background and purpose, this rule of law regulates only such cases in which solely the (purely technical) handling of data processing is assigned to a third party, while the principal continues to handle exclusively the full scope of the actual subject matter involved in discharging the tasks and is thus to retain responsibility for data protection. Whenever duties or tasks pertaining to concrete subject matter are transferred as well as data processing tasks – replies to citizens’ inquiries using prepared text modules, for example – Section 11 of the Federal Data Protection Act alone cannot provide an adequate legal basis, as this in no way constitutes a general legal basis for the transfer of duties. In the relevant literature, a distinction is thus made between permissible data processing on commission and transfers of functions which are not covered by Section 11 of the Federal Data Protection Act. In practice, this leads to obvious difficulties when it comes to distinguishing between these two categories, however.

The eGovernment working group at the Conference of Commissioners for Data Protection of the Federation and the Länder has thus set up a study group headed by myself and charged with evolving potential solutions in this area, as outsourcing and inter-agency projects are acquiring ever greater importance against the background of administrative modernisation and e-government. No concrete results had been achieved at the time of going to press. I will be devoting special attention to these matters in the coming reporting period, however.

### **3 Europe and international affairs**

#### *How to maintain data protection in a globalised world*

Electronic data transfers do not stop at national borders. On account of increased trade volumes, governmental co-operation projects and rising individual mobility, i.a., more and more personal data are communicated across borders. The globalisation of information exchanges requires international data protection standards, as was noted by the 27<sup>th</sup> International Conference of Data Protection and Privacy Commissioners in Montreux in 2005 (cf. 3.5). At the same time, governments and parliaments need to safeguard citizens' rights in the international information society. We expect the European Union to keep up its lead role in data protection matters. The 1995 European data protection directive has defined criteria which are meanwhile accepted in many parts of the world. With this in mind, the EU should define criteria also for the areas left out as yet. It should not curtail data protection rights as part of what they may call the "bureaucracy dismantling" or the "war against terror". Democratic societies need to uphold their principles in particular in difficult and conflicted times. This is also true for data protection.

#### **3.2.2 The Prüm Treaty**

*The Prüm Treaty on cross-border police cooperation was signed by seven EU Member States on 27 May 2005.*

The negotiations which had been initiated by the Benelux states, Austria and Germany in 2003 have thus been concluded (cf. 20th Annual Report, no. 3.3.2.3). France and Spain joined in during the final negotiating stage. Towards the end of the period under review four other EU Member States expressed an interest in acceding to the Treaty, these being Finland, Italy, Portugal and Slovenia. The first states to ratify the Treaty were Austria and Spain, followed by the Federal Republic of Germany. The Treaty took effect between these contracting partners on 23 November 2006.

I generally welcome the approach of the Treaty, but have nevertheless pointed out some data protection deficiencies during the parliamentary discussion. These are primarily that the provisions on mutual access by the contracting parties to the databases held by other partners do not sufficiently accommodate the proportionality principle. For this reason I required what I call a „severity threshold“ in particular with regard to the access to DNA analysis datafiles, restricting access to investigation into serious crimes. Regrettably, this demand has not been met. I hope that the application of the Treaty will in the long run lead to a harmonisation of regulations and methods of criminal law and criminal procedure law.

Before the phased information exchange envisaged in the Treaty is launched, the information technology used by the participating authorities and the complementary implementing agreements need to be harmonised (Article 44 of the Treaty). To this end, several working parties have been set up. The Implementing Agreement was signed by the contracting parties

on 5 December 2006. Unfortunately, the amendments which were demanded by the data protection commissioners of the contracting parties at a meeting in Bonn in July 2006 have not been accommodated. Austria and Germany intended to begin the electronic exchange of DNA data after that.

According to the Treaty, the independent data protection authorities of the contracting parties may check the lawfulness of the transmission or receipt of personal data. For this reason, their cooperation needs to be stepped up significantly. To this end, they are to be provided with logging and documentation data. The Treaty provides that the searching body and the body administering the file need to log and record any transmission and any automated receipt of data. This is a key element of a comprehensive chapter on data protection (cf. box on no. 3.2.2).

A committee of ministers will decide on the implementation of the Treaty pursuant to Article 43 of the Treaty. I had proposed to consult the independent data protection commissioners on data protection safeguards prior to such decisions. Regrettably, this proposal has not been heeded. For this reason it is all the more important that the Treaty be subjected to an evaluation in terms of data protection from the outset, in order to strike a balance between the interest in sharing information and civil rights. This is the aspect I will focus on. Should more states accede to the Prüm Treaty, the question of transposing it into the legal framework of the European Union will arise. In this context, too, the Framework Decision on protecting data processed in the context of police and judicial cooperation is very important (cf. no. 3.2.1).

Box on no. 3.2.2

### **Main contents of the Prüm Treaty**

The Prüm Treaty serves to step up cooperation among the contracting states to combat

- terrorism,
- cross-border crime,
- illegal migration.

For this purpose, the exchange of information, including personal data, will be stepped up, i.a. through

- mutual access to dactyloscopic index data files in what is referred to as hit/no hit procedures,
- mutual access to DNA index data files in what is referred to as hit/no hit procedures,
- mutual direct access to national vehicle registration data,
- preventative communication of personal data during major events with a cross-border dimension,
- communication of personal data to prevent terrorist offences.

So as to safeguard civil rights, the contracting parties undertake to respect a high level of data protection; this includes

- uniform minimum data protection standard,
- principles of purpose with regard to communicated data,

- high quality of communicated data,
- recording and logging of communicated data to enable data protection checks,
- rights of the data subjects, i.a. the right to access and damages.

### 3.2.3 Europol

The European Police Office, EUROPOL, was set up in 1999 to assist EU Member States in combating serious forms of international organised crime. The office seeks to improve cooperation among Member States in order to prevent and combat terrorism, drug trafficking and other forms of serious international crime. In particular by assisting the sharing of information among Member States with regard to automated information compilations. In the meantime EUROPOL has become the most important tool of European-wide police cooperation. In 2006, EUROPOL launched an automated information system into which data can directly be fed by Member States. These are data concerning convicted and accused persons and persons who are thought likely, on account of serious facts under national law, to commit criminal offences with which Europol would deal.

The Joint Supervisory Body, which consists of data protection representatives from the EU Member States, checks whether EUROPOL complies with data protection provisions.

### 3.2.4 Schengen

Nowadays, we take it for granted to take the car or the train from Germany to France or Italy without being checked at the borders. For many of us, “Schengen” stands for the freedom of movement in Europe. Schengen is the name of the small Luxembourg town, where the Convention Applying the Schengen Agreement was concluded in 1990 and in which the contracting parties agreed to remove internal borders. At the same time, they agreed to set up a common information system (SIS) to make it possible to conduct cross-border searches for persons and objects in what was begun to be called the Schengen states. The further development of SIS and the use of the data stored in its context continue to raise data protection concerns.

#### 3.2.4.1 SIS II

*It is planned to replace the existing Schengen Information System by an extended system. The relevant legal basis was adopted by the JHA Council and the European Parliament in December 2006.*

The Schengen Information System was launched in 1995. It will be extended to form the second-generation information system (SIS II) to accommodate the enlargement of the EU and technical progress made (20<sup>th</sup> Annual Report, no. 3.3.2.1). This requires a new legal basis to account for new functions and larger data volumes.

On 31 May 2005, the Commission presented the following proposals to this end:

- Proposal for a Council Decision governing the establishment, operation and use of the second-generation Schengen Information System (SIS II)
  - COM (2005) 230 final



- Proposal for a Regulation of the European Parliament and the Council governing the establishment, operation and use of the second-generation Schengen Information System (SIS II)
  - COM (2005) 236 final
- Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates
  - COM (2005) 237 final

These proposals would replace the provisions which have so far formed the legal basis for SIS (Art. 92 through 119, CAS). Separate legal provisions are necessary because some SIS alerts come under the Third Pillar (police and judicial cooperation in criminal matters), while others come under the First Pillar (Title IV of the Treaty establishing the European Community). The proposals would largely uphold the concept underlying SIS. However, the system would no longer be operated by Member States. The Commission would be charged with what is referred to as operation management, until it is transferred to an agency. Responsibility for alerts in terms of data protection would continue to rest with Member States.

So as to prepare the discussions in the Council and the European Parliament, the Joint Schengen Supervisory Board submitted an opinion with regard to data protection issues on 6 October 2005. The same applies to the EDPS and the Article 29 Working Party.

In its opinion, the Joint Schengen Supervisory Board welcomed the priority given to data protection; however, they also raised general concerns:

- They feared that SIS would in the future be used for extended purposes, and that it might be enlarged to form a comprehensive police information system. This would have to be accompanied by relevant amendments to the legal safeguards.
- They stated that the proposals failed to clearly indicate responsibilities in terms of data protection. This was important, however, to check the lawfulness of data processing in the system.
- The third issue raised concerns the control of SIS II under data protection law. So far, the Joint Supervisory Body has been charged with counselling, controls and coordination – tasks which are no longer contained in the proposal. In addition, the proposal emphasized data processing checks at the central level, which were however minimal, they held. Controlling the personal data processed in SIS II would continue to be incumbent on the national data protection commissioners, they said, for which reason there continued to be a need for coordination.

The discussions in the European bodies were overshadowed by ever new problems related to the bid for tenders and the development of the SIS II project, and took until autumn 2006. At the same time numerous technical and organisational problems had to be solved. The European Parliament and the Council could not agree until the final moment whether or not the intelligence agencies were to be given access to specific alerts in the SIS. An approach I had strictly opposed owing to the lack of transparency in these agencies and on account of the fact that their tasks are not of a police nature. As the European Parliament opposed the opening of SIS to intelligence agencies, the Council dropped this issue, paving the way for the approval of the legal instrument on the basis of the EP compromise proposal. This, however, only settled the legal basis. The issues which were controversial till the end included the integration of biometric features, i.e. fingerprints. It was agreed to first of all use these features only for verification purposes.

The project is vital to make up for the removal of checks at the borders with the new Member States. Given the current state of play, however, also from the technical point of view, it cannot become operational between the old contracting parties before 2008. The new Member States would be connected at an even later date. As this can hardly be sold in political terms, the Council agreed in December 2006 to launch what is referred to as SISone4all (SIS I+ all), which amounts to an extension of the existing SIS I+ to the new acceding countries as of July 2007 without the new features of SIS II. If the operation of SIS I+ is successful in the acceding countries, the controls at the internal borders between the old and the new EU states may be removed in the period from December 2007 to March 2008. In parallel, those responsible will push for the development of SIS II.

The process will need to be guided in terms of data protection before the new functionalities go live (i.a. connecting alerts), extended data catalogues (i.a. biometric features such as photos and fingerprints), and extended access (Europol, Eurojust). Together with my colleagues in the other Member States I will seek to ensure that the new SIS II will strike a sound balance between police search requirements and civil rights.

### **3.3. The Data Protection Working Party pursuant to Article 29 of the EU-Data Protection Directive**

*The Article 29 Working Party has become one of the most important European cooperation committees in the area of data protection*

Pursuant to Article 29 of the EU-Data Protection Directive 95/46/EC the Working Party gives advice to the European Commission and examines the implementation of the Directive into national law in order to achieve a harmonised application of law. It gives statements on the level of data protection in the European Union and also in Third Countries, it adopts working papers in order to draw the attention to particular problems in the area of data protection law and it issues recommendations for the protection of the private life of the citizens living in the European Union.

In the period covered by the report, the Working Party has adopted as a whole 26 working papers dealing again with a wide range of subjects. In this connection, main points were the transfer of air passenger data to the USA (cf. No. 3.3.2), the transfer of data of bank customers to the USA by the Belgian industrial cooperative SWIFT (cf. No. 9.4), the storage of telecommunications data (cf. No.10.1) and data protection in the so-called Third Pillar. Data protection aspects related to electronic health records (cf. No.4.1) and the enforcement of data protection provisions in the health insurance sector (cf. No. 3.3.4) have been dealt with as well. In addition, the Working Party considered the eCall project whose concrete introduction is imminent (cf. No. 12.2), and the storage of personal data on RFID-chips (cf. No. 4.3).

The question of guaranteeing an effective data protection when governmental bodies intend to use data, which had previously been collected by private companies in connection with their customer relations, for law enforcement purposes, was another focal subject of the work of the Working Party. For example, this issue concerns data generated when using telematics in motor vehicles, booking a flight or when telephoning. In this context, it has proven to be particularly problematic that up to now, there still does not exist any legal instrument which regulates data protection in the Third Pillar, thus in the area of justice and law enforcement. This is the reason why the Working Party has repeatedly demanded to finally establish such a

legal framework. Also in the future, the institutions of the European Union will give priority to ensuring that data protection will be respected adequately in all areas of life.

Moreover, the Working Party has focused in particular on a continuous exchange of opinions with representatives of the private sector and with other stakeholders, for example, by carrying out a public consultation before adopting the working paper on RFID (WP 105, see below No. 4.3). The procedure when applying Binding Corporate Rules was also being discussed with representatives of the business sector. These rules are supposed to facilitate considerably the transfer of personal data into countries without an adequate level of data protection. After the conclusion of the voting procedure in spring 2007, it is expected that the elaboration of BCR- application forms that are harmonised at EU-level will begin. Other important subjects were the commitment of companies to inform their clients adequately about their rights of data protection, (so-called Short Privacy Notices), the protection of intellectual property and the data protection aspects concerning whistleblowing in companies in the fight against corruption and falsification of accounts (cf. No. 3.3.1).

In March of 2006, after the expiry of my first two-year term of office, I was re-elected Chairman of the Article 29 Working Party. Also my representative, the President of the Spanish Data Protection Authority, Professor José-Louis Piñar Mañas, was confirmed in his office.

### **3.3.1 Whistleblowing – How to deal with tip-offs from insiders**

*Internal processes to report shortcomings in companies – also referred to as whistleblowing hotlines – need to meet data protection standards*

Numerous companies have launched hotlines for employees to raise concerns which for instance regard billing, auditing, corruption, banking and financial crime and breaches of in-house codes of conduct ethical guidelines. These hotlines have been set up because they are required by law, but also because companies have an interest in identifying unlawful or unethical conduct.

In the USA, for instance, publicly-traded companies covered by the Sarbanes-Oxley Act (“SOX”) are required to make available to employees an anonymous whistleblower reporting system to raise concerns with regard to dubious accounting or review practices. European companies traded at US stock exchanges had to fulfil these requirements by spring 2006. The companies needed guidelines as to how to implement these whistleblowing reporting systems in line with data protection provisions and without clashing with the European data protection directive 95/46/EC. For this reason, the Article 29 Working Party published a working paper dealing with this issue (WP 117/1 February 2006).

The conflicting interests between the person reporting concerns and the person being reported is to be solved in a manner sufficiently accommodating the data protection interests of either side. In the above-mentioned paper, the Article 29 Working Party limited itself first of all to billing, auditing, corruption, banking and financial crime, and drafted related demands (cf. box on no. 3.3.1)

In Germany, an ad-hoc working party of the Düsseldorf Circle dealing with the protection of employee data has also addressed whistleblowing. It is preparing a report to assess whether the collection, processing and use of data in the context of whistleblowing reporting systems is lawful and in line with the Federal Data Protection Act.

You can download the paper submitted by the Article 29 Working Party at [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm).

Box on no. 3.3.1

**Requirements established by the Article 29 Working Party with regard to whistleblowing**

- Employees must be informed about the introduction, purpose and scope of the hotline.
- The scope and the group of persons affected need to be strictly delimited. The information must not be used for other purposes.
- Reports in a person's own name are preferable to anonymous reports; it must be guaranteed that the information about a person reporting a concern is treated confidentially; anonymous reports should be restricted to exceptional cases.  
.
- The principle of proportionality needs to be respected; this means that only the information required for further processing the report may be retained.
- The data needs to be deleted as soon as possible, at the latest two months after the conclusion of the examination. Longer retention periods are only permissible where further legal action is required.
- The person accused is to be informed as soon as there is no risk that evidence may be destroyed. The person reported may generally not be informed of who made the report unless false accusations were made deliberately.

### 3.3.2 The Transfer of Air Passenger Data to the USA

*Also the interim agreement with the USA on the transfer of air passenger data raises data protection questions*

In May 2004 the European Union concluded an agreement with the USA on the transfer of air passenger data. The European Parliament subsequently filed a lawsuit against this agreement with the European Court of Justice (cf. 20th activity report No. 22.2). By its judgment of 30 May 2006 the European Court of Justice decided that this agreement has to be cancelled by the end of September 2006 at the latest due to a lacking legal basis. Following this judgment, in October 2006, a follow-up agreement was negotiated which is valid until 30 July 2007. Previously, the Article 29 Working Party spoke out against the conclusion of bilateral agreements in order to avoid a non-harmonised application of the European Data Protection Directive and an ensuing weakening of the rights of the passengers concerned. Therefore, in principle, I welcome this follow-up agreement, since otherwise, passenger data would have been transferred to the US-Department of Homeland Security without any legal basis and without any contractual safeguards. During the negotiations about the new agreement, which is in numerous details identical to the previous one, one of the results achieved is that the undertakings given by the USA in remain valid. However, the reservations about vital points voiced already by the Article 29 Working Party when concluding the first PNR-agreement remain. This concerns in particular the purpose limitation, which as before has not yet been exactly defined, but also the volume of data that have to be transferred, which could comprise up to 34 elements. Already in previous opinions, the Article 29 Working Party favoured a limited data set of 19 elements, since those elements are considered sufficient in the fight against terrorism.

Until the end of 2006, the shift from a recall procedure (pull) to an active one transferring data on a push-basis as already stipulated in the original agreement has not yet been realized. As before, US-authorities receive data by pulling them which means by having access to the airlines' reservation systems, and by doing so, they can access the complete data set available of each individual passenger. In individual cases, even more than 34 data elements could be accessed. Already the agreement of 2004 foresaw to change the transfer into an active "push" procedure in order to guarantee that sensitive data are filtered out by using a filter software. After the European airlines have repeatedly communicated that the conditions for transferring data by the "push"-procedure have been fulfilled, now, there do no longer exist any plausible reasons for a further delay of the shift. Therefore, the Article 29 Working Party has repeatedly called on the contracting parties to commit themselves immediately to finding a respective solution. It will be the task of the German Council Presidency in the first half-year of 2007 to negotiate a new long-term PNR-agreement, which will take data protection adequately into account and guarantee air-passengers rights and freedoms in the future.

Box on no. 3.3.2

#### **Requirements to a new PNR-agreement**

Also the follow-up agreement with the USA must guarantee an effective protection of the European citizens participating in transatlantic flights. In this connection, the agreement between the EU and Canada could be taken as an example.

- Strict purpose limitation of the data transferred to the fight against international terrorism and the severe cross-border crime. Restriction of automated access to data to the US-authorities competent for controlling entries into the country.
- For compliance with the purpose limitation: Restriction of the transferred data elements to the data required for identifying travellers and for carrying out controls of entry. In this regard, the 19 data elements proposed by the Article 29 Working Party and the 25 data elements agreed with Canada serve as points for orientation.
- Airlines are only allowed to use an active transferring procedure (push) in which sensitive personal data are filtered out.
- Guarantee of an adequate data protection standard when processing data in the USA, in particular ensured by an independent data protection audit and joint regular audits in cooperation with the European data protection authorities.
- Erasure of data after the expiry of an adequate storage period.
- Guarantee of individual data protection rights, in particular the right of information and rectification.
- Limitation of the agreement and inclusion of an assessment clause in order to make it possible to examine whether the agreement is effective and in how far it restricts fundamental rights. This examination has to be carried out according to academic criteria in cooperation with independent experts in due time, before the expiry of the period.

### **3.3.3 The Implementation of Directive 2004/82 EC on the Transfer of Air Passenger Data**

*Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data has not yet been transposed into national law although the respective deadline has already expired on 5 September 2006.*

Also in the EU it is intended to use air passenger data collected by air carriers in order to mitigate the risks of international terrorism. However, in the period under report, the pertinent Directive (API-Directive Abl. L 261/24 of 6 August 2004, cf. 20<sup>th</sup>

Activity Report No. 3.3.5) has still not been transposed into national law. The draft bill presented by the Federal Ministry of the Interior (BMI) in July 2005 was not granted cabinet maturity.

In an opinion on the API-Directive (WP 127 of 28 September 2006) the Article 29 Working Party (cf. No. 3.3) has criticised that this Directive leaves too much scope for divergent interpretation and implementation. Therefore, the Working Party called on Member States to use their scope of discretion while maintaining a well-equilibrated balance between the fight against illegal immigration and the right of data protection.

In autumn 2006 the Federal Ministry of the Interior proposed a new draft bill on air passenger data during the departmental voting. This draft bill envisages the implementation of the Directive by amending the German Federal Police Act (BpolG). Although this idea is to be welcomed, the draft bill meets with considerable concerns for reasons related to data protection aspects:

- It is true that the personal scope of application of Directive 2004/82/EC applies to all air passengers, therefore, also to EU-citizens. However, in order to take the regulations of the Convention implementing the Schengen Agreement into account, the Act should be restricted to transports of third-country nationals via the external borders into the federal territory.
- The list of data that have to be transferred by air carriers exceeds by far the data catalogue of the Directive. In my opinion, copying the page of the identification paper containing the photograph is particularly problematic.
- The transferred data should be deleted by the Federal Police within 24 hours after the entry of the respective plane unless the Federal Police do not require these data for performing their legal tasks incumbent on them. Such an opening clause, which, from a data protection point of view, constitutes a very wide-ranging permission of purpose modification, seems disproportionate to me and I am also of the view that it is irreconcilable with the principle of clear norms. Given the Federal Police's wide range of tasks (cf. Sections 1 to 13 BpolG) I have advocated the restricted use of the data in line with the Directive's objective, which aims in particular to improve the control of entry and fight illegal immigration.

At the time of going to press, the departmental voting on the draft bill had not yet been closed. With regard to this matter, I will take care that the data protection issues will be adequately taken into account.

### **3.3.4 Europe-wide data protection audit in the health insurance sector**

*The first Europe-wide audit in the health insurance sector underlines the importance of such a joint action by national supervisory authorities.*

In March 2006 the Article 29 Working Party launched a Europe-wide initiative with the aim of scrutinizing in joint cooperation with all European Member States the application and implementation of data protection regulations in the health insurance sector. By that action, it was intended to get knowledge about the way personal data are collected and processed by that sector in order to draw, if necessary, conclusions for further measures. That sector was chosen because it concerns a very large part of the population and because it collects

particularly sensitive data of insured persons. Previously, the Article 29 Working Party agreed on a questionnaire which was sent to representative companies and sector associations. Also representatives of the European Association of Insurance Companies were involved in the preparatory work of this action. From the German side 5 insurance companies covering together at least 50 % of the market were involved.

For the Article 29 Working Party such a jointly coordinated Europe-wide audit is of vital importance. This audit shows that the supervisory authorities of the EU-Member States not only cooperate closely, but are also able to impose jointly developed positions on data protection. For the companies concerned, this joint action stressed that the regulations on data protection are implemented in a harmonised way in the European territory. Finally, by this action, the insured persons' awareness of data protection was raised and they were informed about their rights. Individual results of this action are expected to be available in the first half-year of 2007.

### **3.4 European and international cooperation in criminal matters**

*Numerous measures have been taken to improve cooperation in criminal matters at the European and international level. However, these efforts must not take precedence over the rights of the individual.*

In the period under review, the exchange of information from criminal records continued to be an important issue (cf. 20<sup>th</sup> Annual Report, no. 7.9.2). Germany, France, Spain and Belgium have launched a pilot project to improve the electronic exchange of information on criminal conviction. This project took up effective operation in early April 2006. I have closely followed what is referred to as the "project to network criminal records" and have not raised any general concerns in terms of data protection. The information exchanged between the national criminal records is the same that was previously exchanged as hard copies, i.e. information for the home countries about the conviction of their own nationals, and – at the request of a partner state – information from the criminal records. What is new is the electronic communication via the TESTA network (TESTA standing for "Trans-European Services for Telematics between Administrations" (cf. 19<sup>th</sup> Annual Report, no. 8.8), which provides sufficient IT security measures. Foreign registers cannot be accessed directly online. In my view, the connection of the existing national criminal records is by far preferable, in terms of data austerity and the rights of the individual, to the establishment of a central European criminal register of convictions as an index data file at the European level as proposed by the Commission in its White Paper (2005 (2005) 10 final).

The European Commission has furthermore submitted a Proposal for a Framework Decision of the Council about the organisation and content of the exchange of information from the criminal records between Member States (COM (2005) 690 final; Council doc. 5463/06). What is particularly concerning here is the provision according to which data transmitted to the requesting state may not only be used for the original purposes but that they may be re-used to a limited extent in order to prevent some immediate and serious danger to public security. This is very problematic primarily because the possible use of the data concerned would be postponed to a time span which is very hard to foresee. On top of this, the proposed use does not come with a sunset date, so that data which have already been or need to be deleted in the criminal records of the requesting Member State might be used to a larger extent than permissible under national law (Sections 51 and 52 of the Federal Central Criminal Register); this means that the provision would be to the detriment of the data



subject. I have raised these concerns vis-à-vis the Federal Ministry of Justice and requested it to raise them in the Council deliberations on behalf of the Federal Government. I will monitor further developments carefully.

The Proposals for Framework Decisions governing the European Evidence Warrant for obtaining objects, documents and data to be used in criminal proceedings (COM (2003) 688 final; Council doc. 15221/02) and specific procedural rights in criminal proceedings in the EU (COM (2004) 328 final; Council doc. 9318/04), which had already been described in my 20<sup>th</sup> Annual Report, have not been adopted as yet.

There is news about the European Arrest Warrant, though (cf. 20<sup>th</sup> Annual Report, no. 7.9.2). In its judgement of 18 July 2005 (file no.: 2 BvR 2236/04) the Federal Constitutional Court ruled that the German Act implementing the Framework Decision on the European arrest warrant and the surrender procedures between Member States (Federal Law Gazette I p. 1748) was unconstitutional and therefore null and void, because the German legislator had not made use of the room for manoeuvre provided by the Framework Decision in order to uphold basic rights. I very much welcome this ruling because it amounts to a general support of constitutional law in the context of implementing framework decisions which needs to be respected also in the course of other third pillar measures. The required new version of the Act to Implement the European Arrest Warrant took effect on 2 August 2006 (Act of 20 July 2006, Federal Law Gazette I, p. 1721).

Furthermore, the Act to Implement the Convention of 29 May 2000 on mutual assistance in criminal matters between Member States of the European Union entered into force (Act of 22 July 2005, Federal Law Gazette I, p. 2189). What was problematic in terms of data protection was the implementation of the provisions contained in the Convention governing what is referred to as spontaneous communications, i.e. the communication of personal information derived from investigations under the codes of criminal procedure which the courts and prosecutors' offices may pass on to other states also in the absence of a request. Here, the German legislator went beyond what is stated in the convention to be implemented by enabling spontaneous communications not only across the EU but worldwide (Section 61a of the Act on International Mutual Assistance in Criminal Matters). However, the original Draft Act did not contain sufficient safeguards against data communication in cases where the receiving state does not ensure an adequate level of data protection. This was a concern I had raised vis-à-vis the Federal Ministry of Justice and the Legal Affairs Committee of the German Bundestag. During the deliberations in the Legal Affairs Committee I managed to bring about data protection improvements. Specifically, the receiving state must have in place an adequate data protection level. If this is not the case, the communication of data may be ruled out to warrant a legitimate interest of the data subject.

## **4 Technological data protection**

### **4.1 The electronic health card: Continuing waiting**

*The electronic health card has yet to materialise. A circumspect approach is preferable to rushing through this important project, however.*

In accordance with the appurtenant legislation, the electronic health card was to replace today's health insurance card by no later than 1 January 2006. The project concerns around 80 million insured persons, 260 health insurance funds, 2,200 hospitals, 21,000 pharmacies and

188,000 doctors. This is the largest IT project in Germany, its scale is vastly greater than that of the lorry toll system with which it is often compared.

In the debate on the introduction of the electronic health card the danger of a “transparent patient” is often raised. In future, health data, which belong to the scope of personal data warranting special protection under the Federal Data Protection Act, will be in a virtual world over which the insured parties have little control. The telematics infrastructure in the healthcare system is intended to provide the technical basis to provide doctors and pharmacists with the necessary, up-to-date information on the patients in their care within their respective fields of work. The intended improvement in medical care must not be accompanied by a loss of data protection, however. The statutory basis for the electronic health card thus contains detailed rules on access in Sections 291 ff. of Social Code V (cf. 20th Annual Report, no. 21.1). The PIN number of the insured patient and identification confirming that the doctor or pharmacist is a member of the medical profession are required in order to access the card. The technical design of the access concept is such that the confidentiality of information on patients is fully upheld, also vis-à-vis and between members of the medical professions (cf. resolution by the Commissioners for Data Protection of the Federation and the Länder, box on no. 4.1). The fundamental principles of data reduction and data economy are also adhered to. The new card does not result in the collection of new medical data, but is intended solely to enable distributed access to the collected data.

The card is to be introduced in several stages. In its initial launch phase, it already contains a photograph of the insured person to prevent misuse and a standard insuree number which is also retained in the event of the insuree switching to a different insurance fund. In the next stage, prescriptions by doctors and emergency data are to be stored on the card. In the final stage, the card is to enable access to data on previously prescribed pharmaceuticals, electronic medical reports and patients’ records. The only compulsory application is the electronic prescription. All other medical data may only be stored with the express consent of the insured person.

The responsibility for the fundamental decisions relating to the introduction, updating and ongoing development of the electronic health card is the “Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH” (gematik), which was established by the leading organisations forming the self-administration body in the health care sector in January 2005. At the end of 2005 the Federal Ministry of Health enacted the “Ordinance on test measures for the introduction of the electronic health card” (Federal Law Gazette I, p. 3128 ff.), which has since been updated by the amending ordinance of 2 October 2006 (Federal Law Gazette I, p. 2189 ff.). The contents focus primarily on stipulating the test objectives, test components and the applications to be tested. The technical components and their interaction are to be examined in a total of four test stages. Following completion of the laboratory tests at gematik and tests in sample environments, field trials have since begun with 10,000 insured persons. In the final test phase which is to follow, the field trials are to be extended to cover 100,000 participants. The amending ordinance expands the scope of the first test phase (off-line deployment of the electronic health card) to include the applications “electronic prescription” and “emergency data record”. I welcome the fact that my suggestion that organisational and technical methods should be included in the tests which will enable insured persons to exercise their rights, such as the right to inspect and delete the data, has been taken up.

The first field trials began in December 2006 in Flensburg and Saxony, covering up to 10,000 insured persons; trials in five other federal Länder are to begin in the coming months. Handling of the card and application of the processes in practice requires to be tested in order

to draw conclusions on the expected level of acceptance among insured persons and service providers. The legislature has defined clear terms of reference for the protection of health data. These must now prove their worth in daily handling. This lends special importance to these tests, in which the insured persons will use the new card to disclose their health data to doctors, pharmacists and hospitals for the first time. Patients will only accept the health card if they are certain that data protection and medical confidentiality are safeguarded. The success of the new health card is crucially dependent on all data protection issues also being resolved effectively in practice. Against this background, I welcome the thorough preparatory work by gematik and the Federal Ministry of Health and am following the trials very attentively together with the Land Data Protection Commissioners.

Box on section 4.1

**69th Conference of Commissioners for Data Protection of the Federation and the Länder in Kiel on 10 and 11 March 2005**

**Resolution on the introduction of the electronic health card**

The Commissioners for Data Protection of the Federation and the Länder are following the introduction of the electronic health card attentively. They point out that, in accordance with the relevant statutory provisions, the data processing which takes place by means of the card must largely be based on the consent of the insured persons. In order to acquire the acceptance which is required among the insured persons to this end, in addition to the legal basis the necessary technical and organisational conditions also require to be established in practice, in order to ensure that both the confidentiality of information on patients and the freedom for patients to choose whether their data is to be stored and transferred are safeguarded.

The insured persons must be informed as to what data processing operations can be performed with the card, who is responsible for such operations and for what purposes they may carry out such processing. The technical design of the concept for access to medical data must be such that in default mode the confidentiality of information on patients is comprehensively maintained, also towards and between members of the medical professions. The insured persons' power of disposal over their data, as called for in the resolutions at the 47th and 50th data protection conferences, must be ensured by appropriate measures, in order to ensure the confidentiality of the concrete electronic communicative relations under the control of the data subjects in accordance with the current state of the art.

Prior to the obligatory blanket introduction of the electronic health card, the procedures and components are to be tested and examined with regard to their functionality, patient-friendliness and conformity with data protection requirements. The tests and pilot trials must be designed such that the results are open-ended to find the most data protection-friendly solution. Premature decisions in favour of certain methods should thus be avoided.

Independent opinions and certifications such as a data protection seal of approval and a data protection audit may be advantageous in evaluating the health card and the new telematics infrastructure. Planned dates for introduction must not result in any compromises with regard to the existing data protection requirements.

## 4.2 Video surveillance

*Video surveillance has become an integral part of our lives. It is omnipresent in many areas – at railway stations, in shopping streets, inside shops and at social flashpoints in towns and cities.*

Video cameras are the most visible form of ubiquitous surveillance. Video surveillance by private parties and public bodies covers entire inner-city areas: At airports, railway stations, in shopping malls, at department stores or banks, members of the public are likely to be under scrutiny by video systems wherever they go.

Video technology is developing apace and its scope of applications is forever expanding. Until recently large and conspicuous, video cameras are now predominantly small and inconspicuous devices. Only a few years ago, video systems stood out on account of their size and conspicuous form. Shops in particular relied on the deterrent effect of video surveillance, sometimes going so far as to use dummies instead of real camera systems. Such efforts are barely worthwhile today. Video technology has not escaped the general drop in the price of electronic systems. Using dummies instead of operational video cameras would thus result in only a minimal reduction in costs. In addition, so-called “dome cameras” are now in use, particularly when it comes to monitoring large areas, such as railway stations. These are cameras which are able to pan through 360 degrees, with a strong zoom function which is able to pick out points of detail even at a distance of a hundred metres. They are concealed under glass domes, making them similar in appearance to ceiling lamps and barely recognisable as cameras.

There are numerous statutory regulations concerned with the admissibility of video recording, including the police acts of the Länder, the law of assembly and the Federal Data Protection Act. Section 6b of the Federal Data Protection Act regulates “Monitoring publicly accessible areas with optic-electronic devices (video surveillance)” (see box on no. 4.2). This provision renders the admissibility of video surveillance dependent on specific conditions in the area of data protection. What many users fail to consider, however, is the fact that the collected data are also subject to the other provisions of the Federal Data Protection Act when they render persons identifiable. The technical and organisational regulations pursuant to Section 9 and the annex then apply, together with the provisions on deletion of the data in accordance with Section 3 para. 4, no. 5.

Box on section 4.2

### **Section 6b of the Federal Data Protection Act**

#### **Monitoring of publicly accessible areas with optic-electronic devices**

(1) Monitoring publicly accessible areas with optic-electronic devices (video surveillance) is allowable only in so far as it is necessary

1. to fulfil public tasks,
  2. to exercise the right to determine who shall be allowed or denied access or
  3. to pursue rightful interests for precisely defined purposes
- and if there are no indications that the data subjects' legitimate interests prevail.

- (2) The fact that the area is being monitored and the controller's identity shall be made discernible by appropriate means.
- (3) Data that have been collected under sub-section 1 above may be processed or used if this is necessary for the pursued purpose and if there are no indications that the data subjects' legitimate interests prevail. They may only be processed or used for another purpose if this is necessary to avert dangers to state security or public safety or to prosecute crimes.
- (4) Where data collected through video-surveillance are attributed to an identified person, this person shall be informed about such processing or use in conformity with Sections 19a and 33.
- (5) The data shall be deleted without delay, if they are no longer needed for the pursued purpose or if the data subject's legitimate interests stand in the way of any further storage.

#### **4.2.1 Video surveillance needs safeguarding, too!**

*A protection profile for video surveillance systems promotes their deployment in compliance with data protection requirements.*

The inspections which I have carried out in the past have shown that not all video systems which are currently in use meet these technical requirements. Against this background, a stipulation of technical and organisational requirements for video systems was long overdue in the context of data protection.

On the basis of experience acquired in the past, listing such requirements in the form of a check list is not sufficient. The technical and organisational requirements have thus been defined by reference to the Common Criteria (CC – a test concept for IT security) and the requirements pertaining to the processing of data which can be related to individuals in video systems have been described in the form of a protection profile. The concept is intended in particular to assist IT users, manufacturers and data protection officials in developing and operating video surveillance systems.

The protection profile specifies a range of conditions which must be met on the basis of data protection requirements and which can be verified in a certification process (cf. box on no. 4.2.1). The specified conditions can also be employed for review purposes and to verify whether the installation of a system has been carried out in compliance with data protection requirements. The protection profile has been certified by the Federal Office for Information Security (BSI) and can be downloaded from my homepage.

Box on section 4.2.1

The protection profile requires a minimum level of security functionality to support the handling of image data in a manner which complies with the relevant statutory provisions. The following requirements apply here:

- Guaranteed deletion of image data (right of the individual to have their personal data deleted) with compulsory statement of grounds;
- guarantee that image data will be deleted automatically on expiry of the permissible period of storage (where image data are to be stored beyond the stipulated storage period, they must be exported from the video surveillance system beforehand);
- provisions regulating access to image data;

- guarantee that pertinent grounds must always be provided for the export of image data and that such exports are to be carried out exclusively by the observer and administrator;
- logging of evaluation, deletion and configuration actions;
- guarantee that image data are processed in the proper manner;
- guarantee of the integrity, authenticity and confidentiality of received image data

The complete protection profile can be retrieved from the Internet at [www.bfdi.bund.de](http://www.bfdi.bund.de).

#### **4.2.2 Video surveillance at railway stations**

*The Federal Police deploys video technology belonging to Deutsche Bahn AG in discharging its duties. A contract for the use of this technology was concluded between Deutsche Bahn AG and the Federal Police in 2006.*

Deutsche Bahn AG deploys video technology at its railway stations to enable a rapid response to any disturbances. As outlined in the 20th Annual Report (no. 5.3.6), the deployed video technology is also used by the Federal Police, which is responsible for ensuring the safety of railway services. In concluding the leasing contract for use of the technology, the Federal Police has complied with my demand that a legal basis should be established which takes the requirements of Section 11 of the Federal Data Protection Act into account.

The bombs found on trains at the main railway stations in Dortmund and Koblenz in the summer of 2006 and the police's success in quickly apprehending the suspects led to calls for video surveillance to be expanded at railway stations and for such systems to be installed in trains as well. I approach such calls with caution, as video surveillance involves observing large numbers of people and recording their image data without a concrete reason. The use of such systems and the resultant benefit to public safety must be balanced against the rights of individual liberty, i.e. the principle of proportionality must be upheld here, too. The fast evaluation of recordings must be ensured, so that current dangers can actually be countered. Video surveillance must be limited to endangered areas. Finally, it is to be ensured that the recordings do not end up in the wrong hands and are used only for purposes which are permitted by law. According to the concept with which I have been furnished, these requirements are largely met.

In the future, I will continue to attach importance to maintaining the appropriate balance between civil rights and the interests of public safety in the face of the more widespread use of video technology and the introduction of new technologies, such as facial recognition systems (no. 5.2.6). Blanket video surveillance must not be allowed in the future either. It would be disproportionate and would impact on people's social behaviour in an unacceptable manner.

### **4.2.3 Video systems pinpoint shortcomings by the body politic, too!**

*In the area of video surveillance I have carried out two inspections within the scope of my remit. The findings have also played an important role in drawing up a protection profile.*

The increasing use of video technology has prompted me to inspect a number of video surveillance systems with regard to compliance with the data protection requirements stipulated in Section 6b (2) of the Federal Data Protection Act (cf. box on no. 4.2).

The German Bundestag operates video cameras at its properties in Berlin (397 in all), the signals from which are relayed to a surveillance centre. Each camera is set individually and is individually controlled via the surveillance centre. The image data are called up at the surveillance centre and viewed for control purposes, but are not transferred from the surveillance system to other parties. On many buildings the cameras are installed such that they are visible, though on the Reichstag building they are not immediately apparent on account of requirements relating to the building's classification as a protected historical monument. The requirements pursuant to Section 6b of the Federal Data Control Act have essentially been met. I did establish problems in the course of one inspection with regard to the area covered by the cameras and their visibility, however. The Federal Data Protection Act requires video monitoring to be made discernible (Federal Data Protection Act, Section 6b (2)). The German Bundestag meets this requirement in various ways – depending on the location of the camera concerned –, in the form of signs, for example. I had my reservations, however, when – as in the area of “Unter den Linden”, for example – the cameras were aimed such as to record parts of the publicly accessible area, e.g. the tables outside a restaurant. The inspection of one camera revealed that every guest in the outside area of this restaurant could be recognised. In response to my suggestion, the administration of the German Bundestag duly arranged for this camera to be activated only in the evening, when it is no longer possible to see inside the restaurant. A further problem area which I identified was the form of the signs indicating this video surveillance system. There is a pictogram specified for this purpose in DIN standard 33450, which is also understood internationally. The written information in German only which has been used on these signs to date does not meet the appurtenant requirements here, particularly as this area is very heavily frequented by foreign visitors. The German Bundestag will use pictograms in accordance with the DIN standard in future.

### **4.3 RFID (Radio Frequency Identification)**

*Computer chips are becoming ever smaller and more compact. Information technology is now applied in dimensions in which it is no longer perceivable by human beings. RFID technology plays a key role here.*

RFID chips are a key component in the computerisation of our daily lives. This technology harbours new dangers. Not only because it is largely invisible to the data subject, but also because it enables a degree of monitoring of our behaviour and movements. In addition to their use in labelling goods, RFID chips are now also employed by public bodies. The new so-called e-passports, for example, contain RFID chips on which it has been possible to store digitized facial images and items of basic data since November 2005 and to read out such data via radio links (cf. 20th Annual Report, no. 6.2). They are also used to identify forgeries and thus to prevent ticket touting, e.g. at the 2006 World Cup (cf. 20th Annual Report, no. 5.3.7). While this technology is safeguarded against misuse to a certain extent, there is a danger that RFID chips may be read out or even altered without the holder noticing.

Blanket introduction entails substantial risks to the right to determine the use of one's personal data. The globally unique RFID identifiers – similarly to a serial number – for the most diverse objects can be combined with one another and with other personal data relating to users – generally without their knowledge or consent. In this way it is possible to create detailed behaviour, use and movement profiles.

Companies are already obliged to inform consumers when personal data are processed using RFID chips. This obligation applies both to the chips themselves and to the identification of read/write devices. When and how the data subjects are informed remains a moot point, however. In the interests of effective data protection, transparency should take effect at a very early stage, i.e. on the product and on the shop shelves, rather than when the customer's data are recorded by a checkout facility.

The consumer must furthermore be able to read out the memory contents of the RFID chips. In the case of RFID chips which are used to label products and packaging, it must be possible for the customer to control the read/write mechanism and to deactivate it as appropriate.

The risks pertaining to RFID are also recognised at European and international level. The potential and dangers of RFID, standards, interoperability, the allocation of international radio frequencies and the future of RFID technology were evaluated at various workshops organized by the EU Commission in 2006 (<http://www.rfidconsultation.eu>). A poll revealed a clear majority of respondents to be of the view that while radio labels may have advantages, this must not be at the cost of privacy.

RFID was also a key topic on the agenda at the 72nd Data Protection Conference of the Federation and the Länder and the conference of the supreme data protection supervisory authorities for the private sector, each of which has adopted a resolution on this matter. The two resolutions essentially state that the business community should draw up binding regulations for the use of RFID chips in order to ensure the swift and effective protection of consumers' interests and should duly comply with these regulations.

This self-regulation must apply to all market participants and be binding. Mere declarations of intent are not sufficient. If the manufacturers and the trade sector fail to implement self-regulation, the legislature must protect consumers' rights in the application of RFID technology. I also consider compliance with certain general conditions (see box on no. 4.3) to be imperative.

The working group "Technical and organisational data protection issues" of the Conference of Commissioners for Data Protection of the Federation and the Länder has also drafted guidelines on the subject of "The use of RFID in compliance with data protection requirements" which consider data protection aspects of RFID technology. These guidelines can be downloaded from my Internet site (<http://www.bfdi.bund.de>).

#### Box on no. 4.3

In order to protect the rights of privacy of data subjects, the following requirements are to be observed:

– Transparency

All data subjects must be informed comprehensively of the application, intended purpose and contents of RFID chips.



– Identification requirement

Not only the RFID chips themselves, but also the communication processes which are initiated by the chips must be readily identifiable to the data subjects. Secret application is not permissible.

– No secret profile creation

Data from RFID chips from different products may only be processed such that personal behaviour, usage and movement profiles can only be created with the knowledge and consent of the data subjects. Where the clear identification of individual objects is not necessary for a certain purpose, no storage of clearly identifying characteristics is to be carried out on the RFID chips.

– Prevention of unauthorized disclosure

The unauthorised read-out of stored data must be prevented by encrypting the data when it is stored and transferred, for example.

– Deactivation

In the trade and service sectors in particular, it must be possible to deactivate RFID chips permanently or to delete the data contained on such chips, especially when data are no longer required for the purpose for which they were stored on the RFID chips.

Figure on no. 4.3

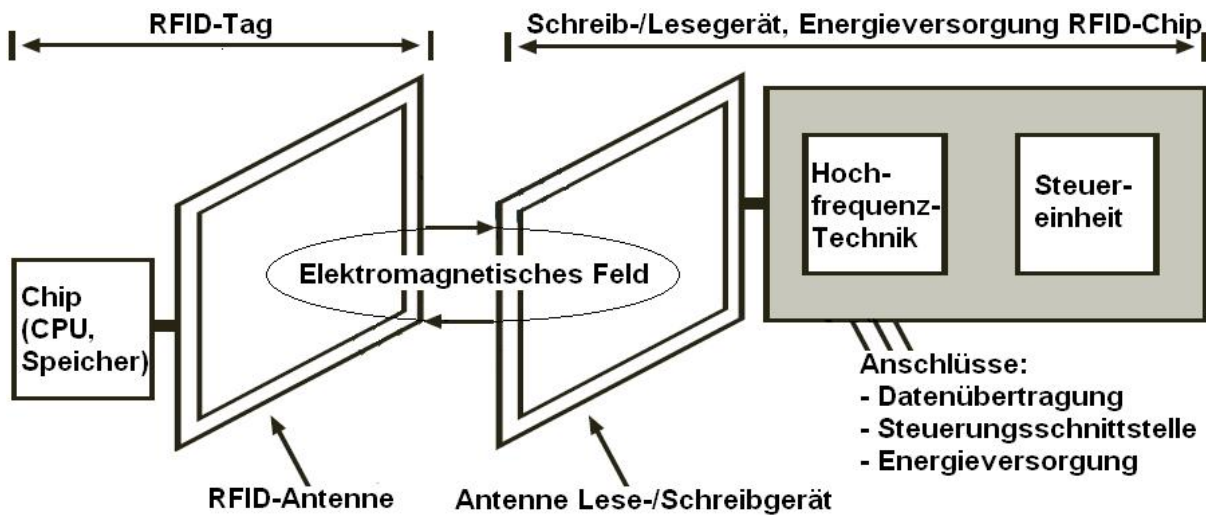
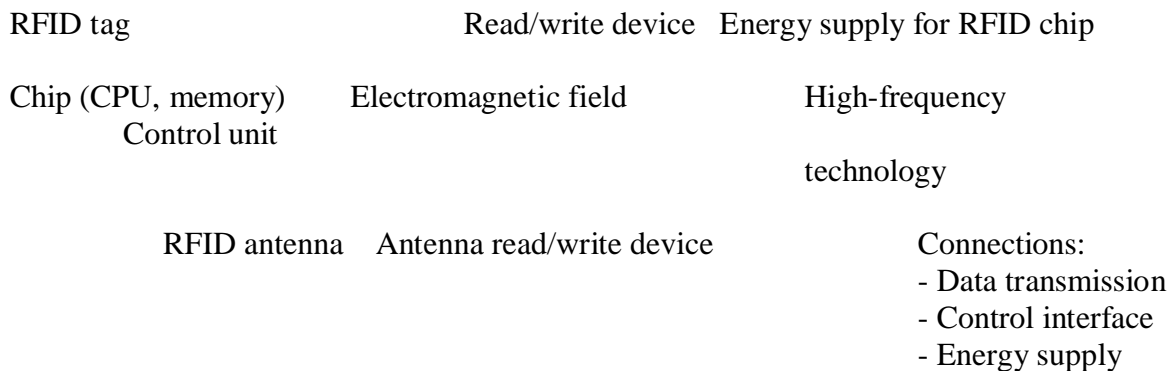


Figure on no.4.3:



## 4.5 Biometrics and data protection

*Biometrics is being used on an ever more widespread basis for identification purposes. This applies to both the public and the private sector.*

Authorities and companies are deploying biometric methods on an ever increasing scale in order to identify individuals and to verify their identity. For some time now, I have thus been concerned with the data protection issues which require to be resolved in connection with the use of biometric characteristics (cf. 19th Annual Report, no. 1.1.1 and 20th Annual Report, no. 4.2.2, for example). The use of biometrics is only justifiable in the context of data protection law when the methods concerned ensure sufficiently reliable identification, the misuse of data is ruled out by technical and organisational measures and the overall process complies with the principles of proportionality and limitation of the use of data to specified purposes. In this context it is also of particular importance that the data subjects be informed of the application and purpose of methods in which their biometric data are evaluated.

The suitability of various biometric methods has been tested at federal level in the period under review. The Federal Office for Information Security was commissioned by the Federal Ministry of the Interior to carry out a study entitled BioP II which examined the recognition performance and anti-violation security of fingerprint, iris and facial recognition facilities. The aim of the study was to examine the performance capabilities of currently available biometric verification systems for application in connection with identification documents. Unfortunately, the competent Federal Ministry of the Interior only furnished me with the complete results of research project BioP II in the autumn of 2005, after insistent enquiry on my part. Furthermore, parts of the report on the results of the study were classified, thus thwarting any possibility of public debate on this information. Such a debate would have been particularly necessary, as the results show that considerable weaknesses still applied in the area of facial and fingerprint recognition. Serviceability studies have also been carried out by the Federal Criminal Police Office (facial recognition in the search project based on photographic images at Mainz central railway station, see no. 5.2.6. below) and by the Federal Police (automated border controls at Frankfurt Airport, see no. 4.5.2 below). I oversaw these projects with regard to data protection aspects.

In addition to official applications, biometric methods are also employed to verify identity for the purposes of access authorisation (generally fingerprint, facial and iris recognition), in payment systems and in verifying passengers' identities (generally fingerprints). In the case of pay systems, both the biometric characteristics and the other customer data (e.g. bank information) are stored in databases. Appropriate data protection and IT security precautions are to be undertaken here to protect the data. As a general principle, the use of biometric recognition systems requires the consent of the data subjects concerned. It remains to be established in the individual cases concerned whether the provision of consent by employees' representatives in works agreements is sufficient in this connection. The users must always be informed as to the technical process, the pursued objectives, the data protection provisions and the risks of the application.

At present, high recognition rates are for the most part only attainable under laboratory conditions. Biometric systems will remain unable to ensure completely reliable facial recognition in the future, too. While mass biometric applications can result in improved comfort and convenience for the user, security and data protection must keep pace with such developments. Additional technical and organisational measures are essential to this end.

#### **4.5.1 Technology**

Biometrics is entering into many areas of our lives. From controls in tourist traffic to identification in supermarket payment systems. It remains doubtful whether the deployed technology actually ensures reliable identification, as is frequently claimed. With regard to fingerprint and facial recognition, progress is to be observed in the areas of anti-violation security and recognition performance, however. The recognition performance of the commercially available fingerprint systems is to be rated as good, for example (provided that the individuals to be verified possess appropriately pronounced characteristics). The major weakness is the vulnerability of the reading devices to manipulation, however. It remains relatively simple to obtain another person's fingerprint and to commit identity fraud with a copy of this fingerprint. A copy of another person's finger can be produced by simple means (keyword "silicone finger"). Even recognition systems featuring so-called "living recognition" offer only a limited protection. Various systems for living recognition are currently being tested, e.g. ultrasonic fingerprint measuring processes or measuring methods in which moisture (perspiration) is included in the recognition process. These systems

promise greater protection against manipulation. In view of the higher costs involved, it remains to be seen whether such fingerprint reading devices will be used in mass applications.

At present, facial recognition predominantly involves two-dimensional measuring methods, whereby an image (photograph) of each data subject is generated for the purposes of comparing facial data and certain facial characteristics from the available image information are compared. The recognition performance of this method is dependent on many external disturbing factors and is thus to be rated as unreliable when these disturbing factors cannot be minimised. The error rate is determined in particular by the quality of the reference image, the lighting and the angle of the head, as well as the ageing process and surgical changes. The introduction of three-dimensional facial recognition is expected to lead to a substantial improvement in recognition performance. This method involves producing a 3D model (relief) of the face. The comparison process is carried out on the basis of the converted facial characteristics. With the 3D method, disturbing factors such as the angle of the head, lighting problems, unfavourable camera angle, distance of the camera from the photographed face or head rotation are minimised, as the computer matches the currently recorded data with the basic data record and then performs the comparison. Potential applications for the 3D technology are the identification of persons for access control purposes and the video surveillance of industrial installations or airports. Possible scenarios for use in combating crime are also under consideration, whereby substantial data protection issues remain to be resolved here.

The European Union (EU) has commissioned a project aimed at clearly identifying persons with the aid of three-dimensional facial recognition. The project, which is entitled “3Dface”, is to run until the end of March 2009. The aim is to deploy 3D technology to render airports safer, to automate border controls and to speed up the check-in process at airports. To this end, 3D facial recognition is also to be combined with surface and texture identification. This is a comprehensive project examining not only matters of operational reliability and protection against forgery but also problems pertaining to the protection of rights of privacy.

#### **4.5.3 The electronic passport and the new identity card**

*The integration of electronic chips into passports and identity cards gives rise to substantial data protection issues.*

On the basis of Council regulation 2252/2004 of 13 December 2004, providing for an RFID chip to be integrated into the passports of EU citizens which, in addition to the data previously contained in a passport – including a digitized photograph – is also to contain fingerprints, so-called electronic passports have been issued since 1 November 2005. Shortly before the end of the period under review, the Federal Ministry of the Interior submitted a draft amendment to the Passport Act which provides for fingerprints to be included in passports also as of 1 November 2007. The Federal Government is additionally planning to introduce a biometrics-enhanced identity card as of 2008.

I reported on the EU passport regulation in my last Annual Report (20th Annual Report, no. 6.2.1). In its resolution on the “Introduction of biometric identity documents” of 1 June 2005 the Conference of Commissioners for Data Protection of the Federation and the Länder expressly welcomed and supported the European Parliament’s commitment to binding minimum standards for biometrics-enhanced passports to prevent misuse, in particular the secret read-out and manipulation of data. At the same time, the Conference noted that the introduction of biometric characteristics entails risks in the area of data protection. To my

regret, the Federal Government ignored the proposed moratorium on the introduction of biometric characteristics into identity documents and adopted the introduction of the so-called electronic passport with effect from 1 November 2005 – again without the adequate involvement of parliament – via the “Second ordinance on the amendment of passport regulations” of 8 August 2005 (Federal Law Gazette I, p. 2306).

The Federal Ministry of the Interior held the view that, on account of the stipulations under European law resulting from regulation 2252/2004, no amendment to the Passport Act was necessary for the introduction of an RFID chip integrated in passports (regarding RFID chips, cf. no. 4.3) in which the data previously printed in passports – including the passport photograph – were to be stored. I took issue with this interpretation. On the one hand, Section 4 (4), sentence 1 of the Passport Act stipulates unambiguously that “the types of biometric characteristics, their details and the incorporation of characteristics and information in encrypted form pursuant to sub-section 3, their mode of storage, other processing and use ...” shall be regulated “... by Federal law” On the other hand, modification of the passport has gone beyond the digital storage of the printed information which was already printed in the conventional passport. The nature of the passport photograph has been changed significantly in Section 3 of the new Specimen Passport Ordinance (Passmusterverordnung), for example. Furthermore, the switch to the digital passport photograph which can be evaluated by automated means represents a significant improvement in quality, with substantial consequences in terms of data protection which ought to have been accompanied by corresponding statutory regulation. The Federal Ministry of the Interior was, after all, of the view that the introduction of fingerprints in passports was not directly inferable from regulation 2252/2004 and that corresponding action was required on the part of the German Bundestag in the form of an amendment to the Passport Act. The Federal Cabinet adopted a corresponding bill a few days before the end of the period under review.

To my great regret, regulation 2252/2004 has deprived the Bundestag of the power to decide on the fundamental question of whether fingerprints are to be incorporated into the passports of German citizens at all. There has been virtually no public debate on the sense and expediency of this rule. The inclusion of such a characteristic is not mandatory on the basis of any stipulations by the International Civil Aviation Organization (ICAO). The proposal for regulation 2252/2004 – in the version in which it was submitted to the European Parliament – only provided for the optional inclusion of fingerprints. In view of the many access systems which are based on the use of fingerprint data, I consider it possible that the risks involved far outweigh the envisaged additional benefits to security.

I appreciate the Federal Government’s efforts to provide extensive protection for the data through technical measures. Doubts remain as to whether these efforts will prove successful, however. The authentication system “Basic Access Control” which has been used for the first version of the electronic passport has already been subject to a number of attempted attacks. Reports have featured in the press not only on the copying of RFID chips but also on attackers gaining access to passport data. I will monitor closely whether security systems deployed to protect the fingerprint data in RFID chips from misuse (e.g. the authentication system “Extended Access Control”) are adequate.

The Federal Government is also planning to incorporate biometric characteristics into the identity card. This is justified first and foremost by reference to the fact that the identity card serves as a travel document within the EU. It is intended to store the same biometric characteristics as are contained in the electronic passport in an RFID chip which is to be integrated into identity cards. Also under consideration is the option of providing a digital certificate pursuant to the Digital Signature Act in identity cards. This certificate could be

activated by citizens, enabling them to furnish digital signatures via the Internet, for example (citizen card function).

The same concerns apply to the incorporation of further biometric data into identity cards as to the introduction of these characteristics into passports, whereby the fact that practically every adult carries their identity card on their person at all times, in contrast to their passport, further reinforces these concerns. In view of the absence of any stipulations under European law requiring the incorporation of fingerprints into identity cards, I suggest that this characteristic should not be introduced into the electronic identity card.

The bill provides for a new clause in both the Passport Act and the Act on Identity Cards, allowing the police authorities and the authorities responsible for public order to carry out the automated transfer of photographs from the passport and identity card registers kept by local authorities in prosecuting traffic offences. From the point of view of data protection, there are no compelling grounds to oppose the automated transfer of photographic data to the police authorities and the authorities responsible for public order in individual instances, in compliance with the requirements of data protection law. The statement of grounds for the bill does not include any cogent explanation as to why an automated retrieval method is required for this purpose, however. According to the original statement of grounds for this provision, the transfer of photographs from the passport and identity card register remains only the final resort, i.e. it may only be carried out where “the data cannot be obtained from the data subject without unreasonable effort or the nature of the task for which the data are required means that such a method of data collection cannot be applied.” It would thus appear that such data transfer does not constitute a mass phenomenon which would justify the authorities accessing the passport and identity card registers online. Furthermore, while the amending act does not result in the establishment of a nationwide file containing biometric characteristics, the right to determine the use of one’s personal data may also be jeopardised by networked databases which correspond to central files from a functional point of view. The planned online retrieval of photographs from the identity card and/or passport register would necessitate networking the involved parties, as even the new statement of grounds in the Passport Act points out. I have thus moved that the planned provision be abandoned.

## 6 The legal system

### 6.1 Line tapping pursuant to Sections 100a et seq. of the Federal Code of Criminal Procedure

*The urgently required reform of the statutory provisions on line tapping in connection with criminal proceedings is finally gathering steam. Regulation is also necessary in the area of so-called cell inquiries.*

The provisions of Sections 100a et seq. of the Federal Code of Criminal Procedure on the subject of wiretapping continue to be in urgent need of reform. I called for legislative action already back in my 20th Annual Report (no. 7.2.1), after the Federal Constitutional Court's judgement of 3 March 2004 on the acoustic surveillance of private homes and scientific studies had revealed substantial shortcomings in the existing provisions. The Federal Constitutional Court has since then again stipulated clear provisions to protect the basic rights of persons under surveillance (judgement of 27 July 2005 on preventive line tapping, cf. no. 5.4.1). At the same time, there has been an alarming rise in cases of telephone wiretapping pursuant to Sections 100a, 100b of the Federal Code of Criminal Procedure (29,017 orders in 2004, 35,015 in 2005, as compared to 24,441 in 2003).

In a joint paper, the Data Protection Commissioners of the Federation and of the Länder formulated the data protection requirements pertaining to the reform of line tapping and other covert investigative measures (box a on no. 6.1) and submitted these to the Federal Ministry of Justice. In November 2006, the Federal Ministry of Justice finally presented a ministerial draft bill for an act to reform line tapping and other covert investigative measures (and to implement the Directive on the retention of data, see no. 10.1 below). The bill is essentially a step in the right direction, in that it strengthens the protection of the rule of law and the fundamental rights in surveillance measures conducted in connection with criminal proceedings. I also welcome the concept for establishing uniform regulations for all covert investigative measures. I have indicated to the Federal Ministry of Justice that I consider amendments to the bill to be necessary on the following points in particular:

- The extensive scope of offences for which line tapping may be ordered for prosecution purposes should undergo a critical review and be reduced in the interests of upholding the privacy of telecommunications.
- In the interest of improved practice with regard to the issuance of line tapping orders, qualified obligations for reasoning are to be incorporated into the act. It must be ensured that the application filed by the public prosecutor as well as the court order are substantiated in concrete terms relating to the individual case concerned.
- I consider the envisaged provisions which are to protect the so-called inviolable core of the private sphere to be defined in too narrow terms in some instances. The intended ban on the collection of data in cases in which exclusively information relating to the core area of the private sphere is to be expected is insufficient. Line tapping should be ruled out as soon as there are concrete indications that the measure will include communications from this private sphere.

- With regard to the protection of confidential relationships, the bill differentiates between spiritual advisers, defending counsels and members of Parliament on the one hand and other persons sworn to professional secrecy on the other. On the contrary, I consider a uniform and high level of protection to be necessary for conversations with all types of persons sworn to professional secrecy (cf. 20th Annual Report, no. 7.4).
- All the intended provisions should be subject to a limited period of validity and undergo an independent, thorough evaluation backed up by scientific findings. This is the only way of ensuring that encroachments on fundamental rights which are unnecessary or no longer necessary are duly reduced or revoked.

I also see a need for regulation in the area of so-called cell inquiries, i.e. requests submitted by investigating authorities to telecommunications service providers with regard to traffic data occurring in a specific radio cell – the smallest geographic unit in a cellular network. This investigative measure to identify an unknown offender is currently based on Section 100h para. 1, sentence 2 of the Federal Code of Criminal Procedure. In view of the intense level of intrusion which cell inquiries entail, particularly on account of the possible large number of uninvolved persons who may be affected, I do not consider this provision, which is incorporated outside of the actual scope of authorisation for traffic data inquiries (Section 100g of the Federal Code of Criminal Procedure) in the strictly procedural rule of Section 100h of the Code, to constitute an adequate legal basis. The Data Protection Commissioners of the Federation and of the Länder have drawn up a joint paper specifying requirements in this area, too (box b on no. 6.1), which I have forwarded to the Federal Ministry of Justice with a request to examine the possibility of revising the current statutory provisions.

In the period under review I also had an opportunity to submit opinions on three constitutional complaints brought before the Federal Constitutional Court from the area of line tapping in connection with criminal proceedings.

- One constitutional complaint concerned the seizure of traffic data which the accused saved on his own PC or mobile telephone after completion of the transfer process. Although the Federal Constitutional Court did not substantiate the special protection of these data on the basis of the privacy of telecommunications, its judgement of 2 March 2006 (ref. no.: 2 BvR 2099/04) represents a welcome continuation of its decisions strengthening rights of privacy, in that it requires special consideration to be accorded to the increased level of protection warranted by these data when assessing the proportionality of state intervention, in the context of encroachment on the right to determine the use of one's personal data.
- Another constitutional complaint centred on Section 100i of the Federal Code of Criminal Procedure (IMSI catchers). The Federal Constitutional Court regrettably declined to consider this matter for a decision by virtue of a chamber resolution of 22 August 2006 (ref. no.: 2 BvR 1345/03), finding – contrary to the view expressed by myself – that no encroachment on the privacy of telecommunications was involved and judging the encroachment on the right to determine the use of one's own data to be not disproportionate. I welcome the fact, however, that the decision expressly calls on the legislative bodies to ensure effective protection of fundamental rights when reforming covert investigative measures.
- The Federal Constitutional Court's decision is pending on the constitutional complaint against the seizure of e-mails which are saved on the service provider's server after completion of the communication process. I await this decision with great interest. In my



opinion submitted to the Court I have pointed out that such e-mails fall within the protective ambit of the privacy of telecommunications until they come to the knowledge of the recipient, after which they are protected by the right to informational self-determination.

Box a on no. 6.1

**Joint Paper of the Conference of the Data Protection Commissioners of the Federation and of the Länder**

**Data protection requirements pertaining to the reform of covert investigative measures (Sections 100a et seq. of the Federal Code of Criminal Procedure)**

The coalition agreement between the governing parties of 11 November 2005 states: "We will revise the provisions on line tapping in the Code of Criminal Procedure with the aim of achieving a harmonious overall regulation of covert investigative measures in connection with criminal proceedings." In this connection, special consideration should be afforded to the following data protection requirements:

1. The scope of the catalogue of criminal offences specified in Section 100a of the Federal Code of Criminal Procedure, which has been expanded at regular intervals since the introduction of the provision, should undergo a review with regard to the nature and severity of the offences. The aim should be to restrict line tapping to serious offences and to consider the actual relevance of the specified offences to practical applications.

In order to ensure comprehensive monitoring of the development of line tapping measures, an obligation to draw up informative reports must be established in the Federal Code of Criminal Procedure. The statistical reporting obligations for operators of telecommunications systems and for the regulatory authorities pursuant to Section 110 para. 8 of the Telecommunications Act must also be retained.

2. The statutory provision for judicial court orders must not be relaxed. In cases in which the public prosecutor seeks expedited orders, the use of produced recordings should be made contingent on a court establishing the lawfulness of such recordings retrospectively.
3. In order to improve the quality of decisions, the provision contained in Section 100b of the Federal Code of Criminal Procedure should be supplemented with the aim to stipulate that the legal basis for orders pursuant to Section 100a of the Federal Code of Criminal Procedure is to be presented in relation to the individual case concerned.
4. The inviolable core of the private sphere which is guaranteed by the right of human dignity is to be ensured. As a general principle, the collection of data is thus inadmissible in this area. Where information concerning the core area of the private sphere is recorded in specific cases, the absolute exclusion of such evidence, a statutory ban on the storage of such data and a requirement to delete such data must be established.
5. In order to protect confidential relationships, a regulation should be established imposing a general ban on the use of conversations between the accused and persons who are entitled to refuse to give evidence, that is, with relatives (Section 52 of the Federal Code of Criminal Procedure), persons sworn to professional secrecy (Section 53

of the Federal Code of Criminal Procedure) and their assistants (Section 53a of the Federal Code of Criminal Procedure).

6. Use of the personal information obtained through the measures is to be restricted to specific purposes, in particular in respect of compliance with the requirements pertaining to their collection. With regard to traffic data which are kept by the telecommunications companies for the purposes of criminal prosecution on the basis of implementation of the EC Directive on the retention of data, this means that such data may only be used for the purpose of prosecuting serious offences – in particular in cases of organised crime and terrorism, as stated in the recitals to the Directive. Section 100g of the Federal Code of Criminal Procedure requires to be revised accordingly.
7. In order to safeguard the restriction of the use of data to a specific purpose, a statutory obligation to identify the data obtained from line tapping measures must be established.
8. The scope of reporting obligations requires to be defined in greater detail in the act. The deadlines for such reports and the judicial verification of compliance with or deferment of such deadlines should be regulated.
9. The above-stated requirements regarding
  - examination of the substantive prerequisites of the measure in the context of the individual case concerned,
  - strict restriction of the collected data to a specific purpose,
  - protection of the core area of the private sphere,
  - greater protection for confidential relationships,
  - the regulation of reporting obligations and deadlines for the deletion of data apply to all covert data collection measures by the prosecuting authorities.

Box b on no. 6.1

**Joint Paper of the Data Protection Commissioners of the Federation and the Länder  
Data protection requirements pertaining to cell inquiries**

1. The Federal Code of Criminal Procedure does not contain a legal basis for cell inquiries with the aim of subsequent automated matching of the transferred data. Such inquiries are thus inadmissible.
2. Even without the aim of subsequent matching, Section 100h para. 1, sentence 2 of the Federal Code of Criminal Procedure, as a procedural provision on Section 100g of the Code, does not constitute an adequate legal basis for cell inquiries, which have become established as a standard police measure for following up suspicions. Encroachments on fundamental rights are always to be reduced to the minimum extent necessary and they require clear and detailed regulation (cf. also decision by the 1st Senate of the Federal Constitutional Court of 4 April 2006 on computer-aided profiling and search, ref. no.: 1 BvR 518/02, paragraph no. 125 et seq.). This is lacking here.

3. Any statutory regulation permitting cell inquiries would have to accord due consideration to the following data protection requirements:
- Cell inquiries within the meaning of Section 100h para. 1, sentence 2 of the Federal Code of Criminal Procedure may only be carried out when a substantial criminal offence has been committed and a sufficiently sound factual basis indicates that the offender has conducted telephone conversations.
  - In the course of an assessment of proportionality for the individual case concerned, the severity of the criminal offence and the number of uninvolved third parties who may be affected by the measure are to be weighed up.
  - The measure is to be limited to the absolute minimum scale necessary in terms of geographic spread and time span.
  - The data obtained on the basis of cell inquiries must not be used to identify witnesses.
  - The call data of the data subjects must be deleted forthwith, as soon as their further storage is no longer necessary for criminal investigations.
  - Statistical records should be kept on cell inquiries, in particular the number of measures, the number of data subjects and the significance of the measures to the investigations concerned, in order to make possible a review of compliance with data protection requirements as well as an evaluation.

### **6.3 Genome analysis in connection with criminal proceedings**

*The act to amend forensic DNA analysis (“Gesetz zur Novellierung der forensischen DNA-Analyse”) of 12 August 2005 layered the barriers to genome analysis in connection with criminal proceedings in a significant manner and established a legal basis for mass DNA screening.*

The discussions on a broadening of the scope of application for DNA analysis in criminal proceedings – with the aim of placing so-called “genetic fingerprinting” on the same footing as conventional fingerprinting pursuant to Section 81b of the Federal Code of Criminal Procedure in terms of the attendant requirements (cf. 20th Annual Report, no. 7.3.2) – continued in the period under review. In response to a bill submitted by several Länder which, for the purposes of DNA analysis to establish the identity of offenders, provided for DNA analysis to no longer be conditional neither on a judicial court order nor for a rescission of the requirement for such analysis to be contingent on a serious offence having been committed and a risk of the future commitment of further severe offences being identified (Bundesrat document 99/05), the Conference of the Data Protection Commissioners of the Federation and of the Länder reiterated its substantial constitutional objections to treating DNA analysis as equivalent to fingerprinting, in a resolution of 17 February 2005 (see box on no. 6.3).

Following this the Federal Government and the coalition parties of the 15th legislative period introduced an “Act to amend forensic DNA analysis” to the German Bundestag, which was passed without amendments and entered into force on 1 November 2005 (Federal Law Gazette I, p. 2360). While this reform does not go so far as to treat DNA analysis absolutely identically to the other criminal investigation measures pursuant to Section 81b of the Federal

Code of Criminal Procedure, it does lower the barriers to DNA analysis considerably in ongoing investigations (Sections 81e, 81f of the Federal Code of Criminal Procedure) and for identification purposes in future criminal proceedings (Section 81g of the Federal Code of Criminal Procedure). In the course of the legislative proceedings I expressed my views to both the Federal Ministry of Justice and the Committee on Legal Affairs of the German Bundestag. My suggestions and concerns were not taken into account, however.

A key aspect of the reform is the relaxation of the requirement for a judicial court order. DNA analysis is now also possible on the basis of the data subject's consent. As such consent is only effective when granted voluntarily, I have considerable doubts whether it will be possible at all to carry out DNA analysis on a relevant scale on the basis of consent, as the data subject will normally be under particular pressure in criminal proceedings. Furthermore, in consenting to DNA analysis for identification purposes in future criminal proceedings, the data subject himself would practically be required to predict that he will not commit any offences in future. I do not believe that the data subject can be expected to make such a prediction. The requirement for a judicial court order is further weakened by the newly introduced powers of the public prosecutor and the police to seek expedited orders. I do not see any practical need for this provision. There are no legally valid grounds why the need to involve a judge in expedited cases should prevent DNA analysis from being carried out in good time. I have no objections to the abolition of the requirement for judicial court orders with regard to the molecular genetic examination of unknown trace materials. I already expressed doubts as to the expediency of court orders in my 20th Annual Report (no. 7.3.2), when the person from whom the trace originates is unknown to the judge.

For DNA analysis for identification purposes in future criminal proceedings, the reform has also lowered the requirements pertaining to the offences giving rise to DNA analysis and the prediction of future offences which may be committed by the data subject. Serious offences or sexual offences were previously prerequisites in both cases. The repeated commitment of non-serious offences (e.g. criminal damage, trespass) now is also sufficient, where the cumulative wrong caused amounts to a serious offence.

It is to be welcomed that an explicit legal basis has now been established (Section 81h of the Federal Code of Criminal Procedure) for mass DNA screening ("mass genetic testing"). This is corresponding to the clarifying definition of the legal framework for this investigative instrument for which I have long been calling (most recently in the 20th Annual Report, no. 7.3.4). Unfortunately, the legal provisions do not clearly stipulate that mass DNA screening is only to be considered as a last resort in criminal investigations and that the group of persons participating in the screening, where it is not clearly defined, is initially to be kept as small as possible, only broadening the scope of the screening in concentric circles if subsequently necessary.

In their coalition agreement of 11 November 2005 (p. 141), the governing parties stated that the act to amend forensic DNA analysis is to be evaluated after two years, thereby examining whether the scope of DNA analysis requires to be broadened for the purposes of criminal investigations. I will be observing developments here closely.

Box on no. 6.3

**Resolution of the Conference of the Data Protection Commissioners of the Federation and of the Länder of 17 February 2005 on the Bundesrat initiative submitted by several Länder on a broadening of the scope of DNA analysis  
DNA analysis should not be treated as an equivalent to fingerprinting**

DNA analysis is an effective instrument in criminal investigations, particularly in cases involving the most serious crimes, such as homicide. This has led to calls for a broadening of its scope of application for identification purposes in future criminal proceedings. A bill submitted by several Federal Länder to the plenary session of the Bundesrat on 18 February 2005, for example, provides for DNA analysis to no longer be conditional on a judicial court order and for a rescission of the requirement for such analysis to be contingent on a serious offence having been committed as well as of a risk of the future commitment of further severe offences being identified.

The argument employed to substantiate such proposals to the effect that DNA analysis can be treated as an equivalent to conventional fingerprinting, is erroneous, however.

Firstly, every human being continuously leaves trace materials in their wake, in the form of skin flakes or hairs, for example. This is one of the reasons for the success of DNA analysis as an investigative instrument, as offenders cannot prevent leaving traces as easily as they can avoid leaving fingerprints. Notwithstanding any careful evaluation of evidence, however, DNA analysis also harbours a heightened danger of uninvolved persons being exposed to unfounded suspicions on account of traces which they happen to have left behind at the scene of the crime, or even of DNA material from third parties deliberately being scattered at the scene of the crime.

Secondly, the current state of the art already permits information beyond that pertaining to the identification of individuals to be obtained from the so-called uncoded segments of DNA (family relationships, probably ethnicity, possibly indications of certain diseases on the basis of the proximity of individual uncoded segments to coded segments). Gender identification is already permitted under current law. And finally it is not possible to foresee what additional findings will be possible in the future in the wake of the expected advances in analytical methods.

It was for good reason, therefore, that the Federal Constitutional Court confirmed the constitutionality of DNA analysis for the purposes of criminal prosecution in two decisions from 2000 and 2001 only subject to fulfilment of the current preconditions of a serious event having been committed, further serious offences being predicted and a judicial court order having been issued. The Court stipulated in particular that these preconditions must also be met in accordance with the circumstances pertaining to the individual case concerned and that their fulfilment is to be carefully examined by the judge.

In view of these decisions by the Court and of the serious encroachment on the right to informational self-determination which DNA analysis represents, the prediction of severe offences and the requirement for a judicial court order must remain preconditions for such measures also in the future.

The special quality of this encroachment on a fundamental right must also serve as a yardstick for all current considerations regarding a possible broadening of the scope of application for DNA analysis. This rules out the possibility of treating the application of this special investigative tool as equivalent to conventional fingerprinting.

## 6.5 Improved enforcement of intellectual property rights – Implementation of the IPR Enforcement Directive

*Intellectual property is to be protected with greater vigour. But at what cost? The plans to oblige Internet service providers to furnish information on customer data do not bode well in the light of the retention of telecommunications data.*

I reported on the so-called IPR Enforcement Directive (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights) back in my 20th Annual Report (nos. 7.12.1 and 7.12.2). Art. 8 of this Directive requires the Member States to ensure that, “in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person ...”.

In order to implement these stipulations, the ministerial draft bill for an act to improve the enforcement of intellectual property rights provides for the incorporation into relevant protective legislation (Patent Act, Utility Models Act, Trade Mark Act, Semi-Conductor Protection Act, Copyright Act, Designs Act, Plant Variety Protection Act) of entitlements to require third parties to furnish information who have not themselves infringed any rights. This is intended to enable the holder of a right to establish the party infringing this right by means available under civil law, so as to enable the holder to enforce his rights more effectively.

This is critical in the context of data protection in particular with regard to the imposition of an obligation on internet providers to furnish information using traffic data as defined in Section 3, no. 3 of the Telecommunications Act, as it constitutes an encroachment on the privacy of telecommunications. Traffic data are all data which occur in the technical implementation of a telecommunication service. These include the IP addresses which are allocated to users for the purpose of surfing the internet. Log files record who is assigned which dynamic IP address, and when. It is thus possible to identify the customer behind an IP address.

In view of the attendant severe encroachment on the constitutionally protected privacy of telecommunications, and contrary to the frequently voiced wishes of the holders of property rights, I consider it imperative that a judicial court order should be required prior to information being furnished. The bill also includes such provision for a judicial court order, but in contrast to the Directive it does not make this contingent on legal proceedings already being pending against the infringer. Rather, the bill envisages the entitlement to information also applying outside of pending legal proceedings, as a means of establishing the identity of an infringing party in cases involving manifest infringements of rights. According to its statement of grounds (p. 82), the Federal Government is focusing here in particular on file-sharing sites “where copyright violations take place on a large scale”.

Even if the protection of intellectual property were to be granted priority in this context, this can only be regarded as proportionate under narrowly defined conditions. Firstly, this applies with regard to the quality of the established infringement giving rise to the entitlement to information. Such an entitlement is only to apply here in cases of infringements which take place on a commercial scale (cf. Section 101 para. 2 of the Draft Copyright Act incorporating the EU Copyright Directive (UrhG-E)). This makes clear that, for example, illegal copying and dissemination on the Internet (e.g. via file-sharing sites) must be on a scale beyond that corresponding to private use and other use for the infringing party’s own purposes.

In assessing proportionality it is of crucial importance, on the other hand, which traffic data may be used. In this connection I have strongly urged for it to be made explicit at least in the legislative intent that this can only be those data which the providers of internet and telecommunication services have stored for their own purposes in accordance with the provisions of the Telecommunications Act (Sections 96 ff.). Access to the telecommunications data stored in accordance with the EU Directive on the retention of data (see no. 10.1 below) must be taboo and, as stipulated by the Directive, must remain restricted to the purposes of prosecuting serious offences (cf. the Resolution of the 71st Conference of the Data Protection Commissioners of the Federation and of the Länder, box on no. 6.5).

I regret the view represented by the responsible Federal Ministry of Justice that a decision on the “highly contentious issue” as to whether and in what form access to such retained data may be permitted should be deferred until implementation of the Directive on the retention of data, and would welcome due clarification as concerns the rules by the legislative bodies at the present juncture.

The contents and scope of the rights and obligations pertaining to both the holders of rights and to providers must be clearly defined in the act. What is more, the holders of rights have expressly wished for the retained data to be included in this entitlement to information under civil law. This confirms my fears. Such a disclosure of telecommunications data – which enjoy the protection as a fundamental right – to satisfy claims under civil law would trigger a course of development which would ultimately result in the virtually boundless availability of such data for myriad purposes. This would be irreconcilable with the principle of proportionality. I thus reiterate my call for corresponding clarification in the act.

I am also critical of the fact that the bill, in contrast to the Directive, does not require a judicial court order in connection with the other entitlements to information from third parties. The largely identically worded amendments to the protective acts (e.g. Section 140b para. 2 of the Draft Patent Act) state that the manifest nature of an infringement is sufficient to legitimize enforcement of the entitlement to information from third parties without a prior judicial decision. I do not consider this proportionate. This would essentially leave it to the third party's discretion to judge whether the conditions pertaining to his obligation to furnish information are met. It would then evidently be sufficient for the holder of the right to present his statement of the facts in a cogent manner in justification of his request for information. I remain unconvinced by the Federal Ministry of Justice's line of argumentation that the requirement for a judicial court order should be waived on account of the large number of requests for information to be expected and the attendant very high strain which would be imposed on the courts. The possibility of a strain on court capacities cannot justify abandoning the principle of proportionality. Furthermore, the very fact that a large number of requests for information are predicted renders application of this rule of law imperative as an obstacle to prevent abuses.

Box on no. 6.5

**Resolution of the 71st Conference of the Data Protection Commissioners of the Federation and of the Länder in Magdeburg from 16 to 17 March 2006**  
**The enforcement of property rights must not erode the privacy of telecommunications**

The Federal Ministry of Justice has presented a ministerial draft bill for an “Act to improve the enforcement of intellectual property rights”, which is intended to introduce more powerful

instruments to protect copyrights and other industrial property rights in implementation of a European Directive.

In certain cases, the bill grants the holders of rights an entitlement to information from uninvolved third parties who have not themselves committed any infringements of copyright. Internet providers, for example, are to be obliged to provide information on data pertaining to their users – information which is currently protected by the privacy of telecommunications. This is intended for example to facilitate the identification of persons offering and using illegally copied music or video files or software.

The Data Protection Commissioners of the Federation and of the Länder caution against the course of development which this would trigger. It is true that the envisaged encroachments on the privacy of telecommunications are tied to formal obstacles in the bill; in particular, the holders of rights are required to obtain a judicial court order. However, the provisions under European law allow Member States such leeway in the interests of data protection that encroachments on the privacy of telecommunications can be avoided. The Federal Constitutional Court has emphasized that scope allowed under Community Law is to be utilised.

Following the increasingly severe and ever more frequent imposition of restrictions on the constitutionally protected privacy of telecommunications for the purposes of criminal prosecution and of secret services in recent years, private economic interests are now to be brought to bear for the first time to impose further substantial constraints. It is to be feared that this will arouse similar desires in other private pressure groups. At the end of this course of development, the data which fall under the constitutionally protected privacy of telecommunications would be available for myriad purposes.

As a result of the entitlements to information from Internet providers, it is to be feared that the obligation to retain traffic data for the very purpose of prosecuting serious offences will be exploited to enforce private interests. In view of the growing tendency for Internet service providers to be made responsible for the contents of their customers' communications, it is further to be feared that the companies will store additional traffic data as a precautionary measure, in order to be able to furnish information in case of infringements of rights.

The Data Protection Commissioners of the Federation and of the Länder thus appeal to the Federal Government and the legislative bodies to refrain from imposing any further constraints on the privacy of telecommunications for the purposes of enforcing economic interests for the first time. It would be totally unacceptable for data the compulsory storage of which has been enforced on the grounds of averting terrorist threats to now be used on a broad scale in the prosecution of copyright infringements. The music and film industries must deploy technical measures of their own and develop new business models to eliminate the essential basis for illegal use.

## 6.6 Digital rights management

*Digital rights management (DRM) must not expose users to a "Big Brother" scenario!*

Copyright is intended to protect intellectual property, whether such property take the form of musical works, films or computer programmes. Only a few years ago it was not foreseeable that copyright enforcement could entail substantial encroachments on data protection rights, particularly with regard to the recording of user behaviour. Digitization always means the



dematerialisation of information. While traditional means of distribution always involved the data being firmly attached to a carrier medium (books, newspapers, films), digitized data can be reproduced without any loss of quality. The possibilities of electronic duplication have considerable consequences on the manner in which copyrighted works are handled. With the technical means available today, even children and adolescents are able to duplicate works or distribute them via the internet, be they in the form of musical works, computer programmes or entire films.

Back in the 20th Annual Report (no. 7.12.2) I covered the draft of a Second Act to regulate copyright in the information society (“Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft”), on which the Bundestag failed to reach a decision on account of the curtailed 15th legislative period. A new government bill (Bundestag document 16/1828 dated 15 June 2006) containing regulations on the system of payment is now under discussion. A welcome aspect is that the flat rate payment system is to be retained as a general principle, thus avoiding the need for the individual registration of each instance of usage. However, the holders of rights are granted the possibility of charging for individual instances of usage as an alternative to the flat-rate charging system. To this end, digital rights management (DRM) systems are to be approved which serve to charge for each individual instance of usage.

While these DRM systems may provide for fairer charging based on actual usage and thus be in consumers’ interests, I have nevertheless highlighted in the course of the legislative process the attendant danger that comprehensive user profiles can be produced with the aid of this technology. The legislative intent contains welcome comments on data protection. Emphasis is given to the principles of data economy, data reduction and system-based data protection, according to which the protection of personal data is to be ensured right from the design stage for the technical systems involved. It is also stated that “Data protection law is subject to ongoing development with due regard to technological advances and the experiences of the supervisory authorities. The possibility is not to be ruled out that the spread of DRM systems and the attendant experience acquired may receive due consideration in data protection law in the future.”

I see this as indicating a heightened awareness of the concerns of data protection. Such fine sentiments alone are not enough, however. It is urgently necessary at this juncture to establish the conditions pertaining to research aimed at ascertaining legal facts, in order to prepare the ground in good time in the interests of users’ rights of privacy. To this end, the further development of DRM and the handling of personal data requires to be overseen on a scientific level.

At the same time, industry and the holders of rights are also to be called on to meet their responsibilities to design DRM in such a manner as to ensure that the mentioned principles of data protection are actually applied in practice. Even in the case of charging based on individual usage, it is quite possible to avoid personal registration. DRM systems could be designed, for example, in such a manner that no registration of usage behaviour is necessary in external databases, when copyrighted works incorporate technical restrictions on use and can only be used within the bounds of the respective licences. Also, as a general principle the individual instances of usage should not be registered and charged for under the user’s name. Alternatively, prepaid models could be applied whereby only usage identifiers and not the users’ identities are registered. Finally, users should, where appropriate, be provided with the option of alternative distribution channels by offering a flat-rate tariff in addition to user-related charging.

## 7 Internal administration

### 7.1 The law concerning aliens

#### 7.1.1 Draft act on the implementation of residence- and asylum-related directives of the European Union

*This bill serves first and foremost to implement residence- and asylum-related directives of the European Union, in addition to which it also provides for further amendments to the laws concerning aliens and asylum. Several provisions give rise to substantial concerns from the point of view of data protection.*

A positive aspect is the fact that a legal basis for the nationalities file (Staatsangehörigkeitsdatei “STADA”) which has been kept at the Federal Office of Administration since 1982, for which I have been calling since the 16th Annual Report (cf. loc. cit. no. 5.7, most recently in the 20th Annual Report, no. 6.8) has finally been established. The bill also contains substantial backward steps in the area of data protection, however.

I am particularly critical of the fact that in the future photographs of all aliens (including EU citizens) are to be stored in the general database of the Central Aliens Register (Section 3, no. 5a of the Draft Act to harmonize the Central Aliens Register with EU legislation – AZRG-E). The Federal Ministry of the Interior has failed to take up my proposal for such storage to be restricted to cases meeting certain conditions, in particular persons whose entry into the Federal territory gives grounds for concern. Although data storage is only to be carried out as of the act coming into force and will not take place retroactively, it is to be assumed that a very large volume of photographs will be stored in the Central Aliens Register within a relatively short period of time. The argument that the photographs are necessary in order to establish the identity of the data subjects is not convincing. Firstly, it ignores the fact that it is possible to establish identities via less drastic measures than the storage of all ID photographs in a central file which is accessible online – for example, via comparison with identity documents and, where appropriate, with ID photographs in foreigners’ files.

Further, it is not apparent why no distinction is to be made between third-country nationals and EU citizens. I would stress once again (cf. 20th Annual Report, no. 6.1.3) that the general storage of the data on EU citizens in the Central Aliens Register is in breach of European Community law. In accordance with Section 2 para. 4 of the Freedom of Movement Act/EU, EU citizens require neither a visa nor a residence title in order to enter the Federal territory. They merely receive a certificate confirming their right of residence from the aliens authority (Section 5 para. 1 of the Freedom of Movement Act/EU). In view of the administrative proceedings pending in this matter and against the background of the treaty violation proceedings instituted against the Federal Republic of Germany by the European Commission (cf. 20<sup>th</sup> Annual Report no. 6.1.4), at least the further storage of data on nationals of EU Member States should be avoided and EU citizens should be exempted from the envisaged regulation in AZRG-E, Section 3, no. 5 a.

In the wake of the failed suitcase bomb attacks in July 2006, the Federal Ministry of the Interior has supplemented the bill. I have conducted various discussions with the Federal

Ministry of the Interior on the need for the amendments “on grounds of internal security”. My doubts remain on two points:

I do not recognise the need for the provision in Section 73 para. 3 of the act to harmonize the Residence Act with EU legislation (AufenthG-E), according to which all data transferred by the security authorities to the bodies involved in the screening process in connection with which no grounds for security reservations are established (non-hits) may be stored by such bodies for the entire period of validity of the residence title. As with regard to the storage of such data in files of the police and the Federal and Länder intelligence services, I also consider the storage of personal data on persons for whom the screening process proves negative to be unnecessary at these bodies. I thus hold the view that the transferred data must be erased after examination.

I also consider it critical that the bill does not maintain the previous graduated procedure for the retrieval of information from the Central Aliens Register. The envisaged possibility of unlimited access for all the authorities specified in Section 15 of AZRG-E alone represents a considerable erosion of data protection. To date, Section 16 of the Act on the Central Aliens Register has provided for a graduated procedure for the retrieval of information from the Central Aliens Register by other law enforcement agencies, public prosecutors and courts. According to this provision, inquiries may be submitted in three stages. In each stage, the necessity of the information to discharging the task concerned is to be reviewed anew; when such information is found to be necessary, the bodies concerned receive further information. In the third and most comprehensive stage, automated retrieval pursuant to Section 22 para. 1 of the Act on the Central Aliens Register is not possible.

In contrast to the arrangements to date, the intended unrestricted and ungraduated access to the Central Aliens Register does not accord adequate consideration to the principle of proportionality. The legislative intent does not provide any cogent arguments to justify the intended abolition of the safeguards in the area of data retrieval which are of substantial importance to data protection. The stated rapid access is certainly not sufficient; such access is already available to the bodies when a corresponding need applies.

I hope that the Federal Ministry of the Interior will take account of my arguments in the further course of the legislative process. No results had emerged at the time of going to press.

## **7.5 2011 Census – The countdown has begun**

*The planned census in 1983 caused a great stir and led to widespread protests among the population. I do not expect the planned new census to prompt any debate on a comparable scale.*

It has been decided that Germany will participate in the EU-wide census round planned for 2010/2011 with a register-based census. The Federal Cabinet passed a corresponding decision on 29 August 2006, on the basis of the results of a trial census run conducted in the period from 2001 to 2003 (cf. 20th Annual Report, no. 6.12). The Federal Ministry of the Interior has since presented a ministerial “Draft bill to prepare for a register-based census, including a census of buildings and housing, in 2011”. This bill primarily regulates the contents and structure of a comprehensive register of addresses and buildings which is to contain all the buildings and homes in Germany and the addresses of all the owners or administrators of all these buildings for the intended postal census of buildings and housing. This file is also to serve as the central instrument for the organisation and support of data collection in

connection with the register-based census, accessible to all processes relating to addresses and buildings. The register will be fed with data from the surveying authorities, the registration authorities and the Federal Employment Agency. Set-up of the register is to be completed by 31 December 2010. The register is to be erased no later than six years after the date of the census.

I have no objections to the concept of the census as such from the data protection point of view.

In my view, a critical aspect in terms of data protection considerations, however, is the planned introduction of a system of georeferencing below the level of the local authority unit or municipal district through the recording for the first time of the geographic coordinates of every individual building. The surveying authorities of the Länder are to transfer these data to the Federal Statistical Office to enable pinpointed presentation of the census results. According to the legislative intent for the bill, the advantage of this georeferencing lies in the possibility of compiling data for small geographic areas according to requirements, without being tied to given administrative boundaries. The bill states that a reliable method of rendering such georeferenced results anonymous has yet to be developed. A type of geographic “grid cell” is envisaged in this connection, instead of coordinates pinpointing specific addresses.

Even at the initial presentation of these ideas by the Federal Statistical Office, I pointed out the dangers which this method harbours with regard to the right to informational self-determination. The diverse use of statistical results gives rise to various means of combining different results and analyses for a geographic reference point, superimposing these one on top of the other in the manner of foils, as it were, to obtain highly informative and comprehensive information on extremely specific geographic units of space. The resultant density of information on small spatial units harbours a high risk of reidentification. This risk is further compounded by the fact that other statistics are also to be georeferenced in the future. This means that it will be possible in the future to combine statistical results from various areas in countless variants for pinpointed applications. This would drastically broaden the typical applicability of collected statistical data for the most diverse purposes. It is also self-evident that pinpointing statistical results will also substantially heighten the risks of individual profile generation (see no. 9.1 below).

The legislative intent of the bill does identify the risks pertaining to georeferencing, referring in this connection to anonymisation methods which have yet to be developed to take account of data protection concerns. Regrettably, the bill does not stipulate any concrete measures to back up such good intentions.

## **8 Financial matters**

### **8.2 Retrieval of account data by tax offices and other authorities**

*Although a decision by the Federal Constitutional Court on the legality of the data retrieval method is still pending, the fiscal administration intends to further increase the volume in 2007 to up to 5000 retrievals per day.*

During the period under review I have repeatedly had occasion to consider the process for the automated retrieval of master account data which was introduced by the “Act to promote tax compliance” at the end of 2003 (cf. 20 Annual Report, no. 8.3).

This enabled the financial and other authorities as well as courts of law to access citizens’ master account data (including name, date of birth, account numbers and number of accounts, but not account balances or movements in accounts) (Section 93 para. 7 and 8 of the German Fiscal Code). It is the Federal Central Tax Office which collects the data.

Since 1 April 2003 banks are required to keep master account data available in separate files. Originally, data retrieval was only permitted in accordance with Section 24c of the Federal German Banking Act for the purposes of combating illegal financial transactions in the area of terrorism and organised crime. The above-stated act has expanded the scope of purposes for which the retrieval of account data is permissible by including the “assessment and collection” of taxes. This measure was justified by pointing out that the fiscal administration must have the means to track down undeclared capital gains.

I indicated the inadequacies of the said act with regard to data protection aspects during the legislative process (see box on no. 8.2). The Federal Constitutional Court has yet to decide on constitutional complaints which were filed against the provisions at the end of 2004. After weighing up the possible consequences, however, in its decision of 22 March 2005 the Court opted not to defer the act by means of a provisional order. As a result the provisions entered into force on 1 April 2005. The deciding aspect here was the fact that the Federal Ministry of Finance had shortly beforehand issued an ordinance on application of the Fiscal Code which was intended to prevent abuse of the procedure and unauthorised data retrieval.

The manner in which the retrieval of account data is actually handled in practice at the authorities requesting information has been examined in various instances by my colleagues at Länder level, while I have scrutinised procedures at the Federal Central Tax Office. A number of deficiencies have been identified in the course of these investigations. The retrieval of account data was ordered by unauthorised persons, for example, forms were not correctly completed or information was missing from the forms and the grounds for data retrieval were not correctly stated, discretionary consideration was not practiced or not documented, data subjects were not informed about the retrieval of their account data or they were not granted an opportunity to furnish the necessary information themselves. The retrieval of account data was also logged in breach of the relevant statutory provisions and more information than was required by the requesting authorities was frequently provided. The data protection commissioners of the Länder and myself have called for a change of this situation. While it has not yet been possible to eradicate all the shortcomings, I am working together with all the relevant bodies on respective solutions. A form has been developed, for example, which enables the conditions pertaining to such a measure to be checked and automatically documented. The Federal Ministry of Finance has since discussed the form with the finance ministries of the Länder, which have for the most part adopted the form.

Furthermore, I consider it problematic that the Federal Central Tax Office does not inform data subjects at present as to whether account data relating to them have been retrieved. The Federal Ministry of Finance holds the view that it is not necessary to furnish such information, as the data subjects are informed as standard practice by the authorities retrieving the data. The Ministry further cites the risk that furnishing such information could jeopardise the purpose of the current investigations, adding that such a risk could only be judged by the retrieving authority, however. This line of argument fails to convince me, particularly as data protection controls have revealed that retrieving authorities regularly omit to inform data subjects on the retrieval of their account data (see above). In addition, it is not apparent how the purpose of the investigations could be put at risk when the account data has already been received. Consequently, the Federal Central Tax Office must furnish the desired information to the data subjects.

The above example demonstrates once again the urgent need for a regulation of the data subjects' entitlements to information by the German Fiscal Code. The data protection commissioners have been raising this requirement for some years now (cf. 20th Annual Report, no. 8.1). While the Federal Ministry of Finance recently indicated a willingness to address this matter, I have yet to receive any draft provisions.

I have further established that in the majority of cases retrievals of account data currently take place not with the aim of uncovering fraudulently concealed capital gains, as specified in the legislative intent, but rather in connection with the enforcement of court judgements. The Federal Ministry of Finance regards the enforcement of court judgements as part of the procedure for levying taxes and charges and thus considers the retrieval of account data lawful in this area, too. It remains to be seen whether the Federal Constitutional Court will share this interpretation of the law.

In the meantime, the fiscal administration has continually raised the number of retrievals of account data. 60 retrievals per day were possible initially, as compared to over 100 today. In 2007, the possible number of retrievals is to be increased to 5,000 a day. In view of the cases pending before the Federal Constitutional Court, I consider this problematic. The Federal Ministry of Finance is considering introducing the final tax which I proposed during the legislative process as an alternative to the account data retrieval method. This would inevitably have consequences for the retrieval process.

Box on section 8.2

**Critical aspects from a data protection perspective**

I see need for improvements in the following areas with regard to the provisions on the retrieval of account information pursuant to Section 93 of the German Fiscal Code.

**Legal clarity**

The provisions in Section 93 para. 8 of the German Fiscal Code do not comply with the principle of legal clarity. It is not stipulated which authorities are permitted to retrieve information for what purpose. Neither is the permissibility of inquiries regulated. The act grants other authorities the power to retrieve information when the statutory provisions which they implement are related to aspects of income tax law, without stating which concrete aspects are concerned. Although seven acts which the Federal Ministry of Finance regards as entailing an entitlement to retrieve data are stated in an ordinance on application of the Fiscal Code (cf. no. 8.2) issued by the Federal Ministry of Finance, this does not conclusively regulate which bodies are able to retrieve data for which purposes in sufficiently clear terms for the data subject. As such, the legal scope of application of these provisions remains too vague.

### **Proportionality**

A restriction of the fundamental right to determine the use of one's personal data is only permissible where this is appropriate, necessary and commensurate, i.e. proportionate, in order to achieve the given purpose. In order to uphold the principle of proportionality, the legislature must establish a commensurate balance between the public interest (uniform and equal taxation) and the individual interests of the data subject (ruling 100, 313, (376) of the Federal Constitutional Court). This has not received due consideration in the act.

It is true that the ordinance on application of the Fiscal Code requires the retrieval of account data to take place in the specific context of the individual case concerned, whereby the competent fiscal authority is to decide on the necessity of data retrieval at its discretion on the basis of a prediction as to the likely results of such a measure. However, this does not rule out the comprehensive retrieval of account data as a "routine" measure when processing a tax return. In order to stem "routine retrieval" in the field of tax data and banking secrecy pursuant to Section 30a of the Fiscal Code, which is a particularly sensitive area in the context of data protection, the act should have regulated who is permitted to order and request the retrieval of account data at the corresponding courts and authorities respectively.

### **Transparency**

A problematic aspect in terms of data protection is the fact that the tax payer concerned does not receive any indication as to the retrieval of account data – at least not initially. The ordinance on application of the Fiscal Code does provide for the data subject to be informed of the data retrieval at a subsequent juncture, e.g. when the next tax assessment notice is sent out. Although this ensures a certain degree of transparency for retrievals pursuant to Section 93 para. 7 of the Fiscal Code, I nevertheless consider a statutory provision to be necessary which stipulates that the data subjects must always be notified in case their personal data are collected, processed or utilised without their knowledge. Such a provision is vital in particular in view of the fact that the ordinance on application of the Fiscal Code cannot take effect in cases pursuant to Section 93 para. 8 of the Fiscal Code because it is not binding on authorities outside of the fiscal administration.

In addition to subsequent notification, I also consider it necessary for data subjects to be informed about the possibility of data retrieval and the attendant conditions prior to such retrieval. This information should also specify the identity of the controller and state the given purposes, processing or use – as stipulated in Section 19a of the Federal Data Protection Act, in order to comply with the data subject's substantive entitlement to concrete and effective judicial control.

### **Preservation of evidence**

The act does not include any obligations regarding documentation. Without corresponding documentation it is difficult for the data subject and the courts to trace the actual course of

events. Documentation should detail who ordered the retrieval of account data, for what reasons, and why this was necessary, for example.

## 9 Business

### 9.1 The need to prevent profiling

*The creation of personality, usage and customer profiles has gained momentum in dramatic fashion, above all as a result of new technologies and the use of new technical means, in particular by information bureaus.*

I have already referred to the problem of profiling in my last Annual Report (cf. 20th Annual Report, no. 11.7). In a resolution dated 17 February 2005 (Bundestag document 15/4597), the German Bundestag called on the Federal Government to examine whether and how the alarming profiling trend might be countered. Unfortunately, no measures have been undertaken in this direction to date. In addition to the growing volumes of data and the diverse options which are already available for linking data, the use of collected data has taken on a new dimension involving the linkage of this data with digital street maps and general maps – a development known as geomarketing. Market researchers link buying behaviour, risks of illness and paying habits with digital maps. In this way, individual profiles are created on the basis of the corresponding addresses, irrespective of whether the information stored in these profiles actually applies to the data subject concerned. Those responsible point out that they are only defining statistical probabilities, not people. Yet here lies the core of the data protection problem: Those who live in the “wrong” place are subject to a blanket negative assessment, possibly with corresponding negative consequences. The law as it stands does not address these problematic developments adequately. It is high time for legislative action here.

#### **Statutory regulation of scoring methods:**

Scoring methods are used to rate customers' economic status on the basis of diverse criteria. Such methods are now applied in virtually all areas of business, and can have far-reaching consequences for consumers: Customers with poor scores receive unfavourable terms; they pay higher interests on loans, are only able to order goods on a cash-before-delivery basis, they are kept waiting longer when they contact call centres and are often refused contracts from the outset. Score ratings are acquiring crucial importance in an ever broader scope of business decisions. People's future buying and payment behaviour is forecast to a substantial extent on the basis of data which do not relate directly to their actual creditworthiness. Apart from information on the data subject's actual behaviour, scores are allocated on the basis of the most diverse data, e.g.



- socio-demographic data (e.g. residential area with above-average number of social welfare recipients; street in which there is a predominance of subscriptions to business magazines);
- neighbourhood analyses;
- representative observations (e.g. real or electronic visits to streets);
- data purchased from the most diverse areas (e.g. car data from the Federal Office for Motor Traffic);
- other empirical data (e.g. nationality, gender).

This means that the individual's creditworthiness is evaluated even in the absence of individual information, e.g. paying behaviour, income and financial circumstances. This largely deprives the data subject of the opportunity to influence his or her public image through his or her own upright behaviour. Furthermore, the lack of transparency of the employed methods prevents the data subject from correcting a "false picture".

This critical trend must be checked by statutory provisions, stipulating that only characteristics of relevance to creditworthiness may be used to calculate scores. A statistical correlation alone does not constitute an adequate condition for incorporation in scoring methods.

It must be apparent to the data subject (and to the supervisory authorities)

- what factors are included in the calculation of the score value, and with what weightings,
- what concrete personal characteristics are used,
- which characteristics have had a negative effect on the data subject's concrete score value. The decisive characteristics should be specified according to their importance and the extent of their influence on the concrete score value.
- furthermore, every data subject should be able to ascertain the score value which has been communicated to a certain contracting party. As a new score value is generally generated each time an inquiry is submitted, it cannot be sufficient to provide the value which currently applies at the time of furnishing information to the data subject.

Only when these conditions are met data subjects will be in a position to check the characteristics, correct them where appropriate, and to explain certain negatively weighted factors to a party with whom they wish to enter into a contractual relationship.

### **Statutory regulation required for the collection of anonymised and georeferenced data**

Technical progress in linking personal data to geographic information (so-called georeferencing) has recently given rise to the problem that on the basis of an address the

knowledge available on this geographic spot (e.g. regional probability of loan default, plotted maps detailing health risks or life expectancy) can be allocated to a person living there. Equally, initially anonymised data can be linked to a certain address, thus attributing these data to people who live there.

The Federal Office for Motor Traffic (KBA), for example, charges list brokers for microgeographic breakdowns of data on car and motorcycle ownership which it supplies on a contractual basis. The list broker provides the KBA with an area-wide file detailing buildings, including microcells (20 households on average). The KBA combines this file with its own data by allocating information on cars and motorcycles to the respective buildings and collating these data with the microcells relating to the respective buildings. The KBA then furnishes this file to the client (list broker).

The list brokers sell the resultant processed and supplemented data to business enterprises, which evaluate them for the purposes of advertising, market and opinion research and to generate customer profiles. The data supplied by the KBA is also included in this scoring method. Even originally statistical data, stating, for example, that 30 % of the occupants of a certain house or a certain address own a certain type of vehicle, remain of a non-personal nature only, as long as this information can only be narrowed down to several occupants or households. When these data are combined with the information that a certain person lives at an address, however, they become personal data allowing the individual allocation of probabilities. The provisions of the Federal Data Protection Act come into play at this instance at the very latest. Requests for information filed by data subjects prior to this juncture have been in vain to date, however, due to the lack of a personal link. The data subject thus remains ignorant as to what information has been included in the score value, how these data have been evaluated and to what extent they have been passed on to third parties.

The combination of originally anonymised information with identification data or with georeferenced data requires to be regulated as a matter of urgency. I consider it necessary to include the use of georeferenced data in the ambit of the Federal Data Protection Act and to ensure due protection in this area.

### **No information to parties bearing no risk as creditors**

While to date the business partners of credit agencies have been limited to the credit- and loan-granting sector (banks, telecommunications companies, mail order companies), these agencies are now increasingly opening up to other business areas which are also interested in their customers' creditworthiness, although they themselves do not enter into any risks as creditors. The SCHUFA credit reference agency for example has included both the housing and the insurance sector in its information system – against the wishes of the data protection supervisory authorities.

In the overwhelming majority of cases, insurance companies do not bear any economic risk beyond general economic risk (in the form of handling charges or profit expectations). On the

insured party failing to pay their insurance premium, the insurance cover lapses. The insurance company is released from its obligation to effect any payments; as a general principle, the company is not required to effect any advance payments. The housing sector hedges against losses of rent by means of advances on rents due.

The ever broader scope of the credit agencies' contractual partners means that personal data on practically all members of the public are spread even more widely. The data subjects' behaviour is being mapped to an increasing extent and without their knowledge or consent. The fact that data from ever more areas are being included in the data pools of credit agencies and can be retrieved from these pools exacerbates the profiling problem. A negative entry in credit agencies' systems, be it justified or not, may lead to the data subject failing to find an apartment or to obtain an insurance policy, for example.

A provision should be adopted into the Federal Data Protection Act, explicitly stipulating that credit agencies may only transfer data to third parties who bear a risk as creditors, so as to avoid a situation whereby any sector of industry, including potential employers, is able to obtain various information on data subjects from third parties which was actually collected for other purposes.

### **Sector-specific information systems**

According to applicable law, data which a credit agency has stored in its system may be transferred to a third party where the latter is able to substantiate a justified interest in obtaining knowledge of the data and the data subject has no interests warranting exclusion of the data from such transfer. This general arrangement has led to credit agencies building up central data bases containing comprehensive information which all of the bureaus' partners are able to access in unfiltered form.

Landlords frequently turn to credit agencies to obtain a general and comprehensive creditworthiness profile on a potential tenant, for example.

Insurance companies, doctors, etc. are also able to check whether their clients or patients have a "clean slate" before entering into contractual relationships with data subjects.

This legal situation requires a clarification so as to replace comprehensive data bases with sector-specific information systems. In order to accommodate the needs of individual branches of industry for protection, they should not be fully deprived of the means of sounding out their potential contractual partners' previous behaviour. The scope of such systems, however, should be restricted on a sectoral basis. This means that a landlord may receive information on whether a potential tenant has been in default in any previous tenancies, for example, but not as to whether he or she has failed to pay an invoice from a mail order company.

Such a sectoral approach has proven effective abroad, e.g. in France, where a comprehensive information system such as the German one is unknown.

## **Entitlement to remedial action**

To date, the data subject has been largely defenceless in the face of electronic warning systems. Complaints show that many citizens end up in electronic warning systems through no fault of their own, as a result of mistaken identity, negligent or incorrect reporting procedures by parties participating in such systems and/or the inadequate verification of reported data by system operators. Even if a data element has been identified as incorrect and has been duly corrected, the data subject does not know to whom the information has already been transferred and what damage has thus already been caused.

Such a situation could be countered by incorporating a statutory entitlement to remedial action into the Federal Data Protection Act. In cases of onward transfers of incorrect information or transfers of information by unlawful means (e.g. disputed claims), this entitlement should require the controller to rectify the consequences for the data subject – not only in its own system but wherever the onward transfer of the error may have negative consequences for the data subject. In concrete terms, this means that the credit agencies would be required to notify all parties to whom they have transferred an incorrect piece of information of the incorrectness thereof. Where the incorrect item of data has been included in a score value, the latter would have to be transferred to the recipient once again in duly corrected form. The recipient would then be required to ensure that any negative consequences for the data subject resulting from the incorrect score value were also eradicated.

## **9.4 SWIFT – Inadmissible transfer of data to US authorities**

*The transfer of data to the USA in connection with international transfer orders constitutes a breach of European data protection law.*

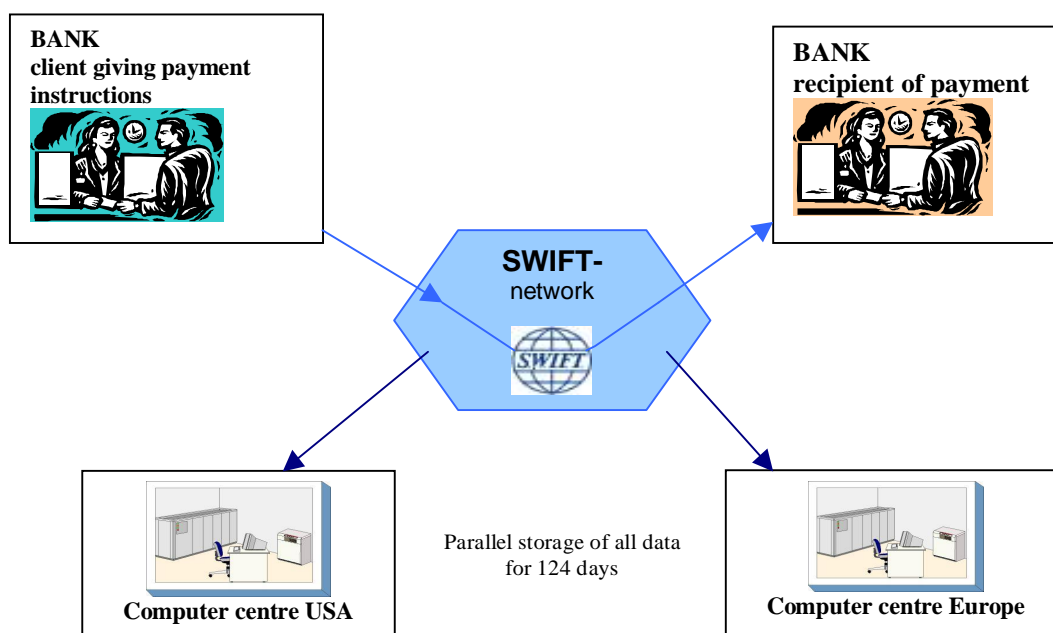
Publications in the media at the end of June 2006 revealed that US authorities had enjoyed access to the payment transaction data of SWIFT (Society for Worldwide Interbank Financial Telecommunications) since 2001, in order to evaluate this information in the fight against terrorism. SWIFT is a co-operative established by the international banking industry under Belgian law in 1973. The transfer orders which are transmitted via the SWIFTNet FIN service contain personal data such as the name of the sender and the recipient. SWIFT stores all transfer data for 124 days at two data-processing centres, one of them is located in Europe while the other is situated in the USA. American authorities have enforced the release of transaction data from SWIFT on repeated occasions on the basis of subpoenas, whereby in all cases the technical and legal point of reference for these orders has been the SWIFT data-processing centre in the USA. In 2003 SWIFT and the US authorities concluded an agreement stipulating the procedure for the transfer of data. SWIFT has subsequently released data

without any judicial review of the cases concerned. As a general rule, SWIFT users have not been informed of such data transfer, its scope or purpose.

The Düsseldorf Circle of German data protection supervisory authorities and the Article 29 Data Protection Working Party of the EU Member States have established that the current mirroring of data records at the data-processing centre in the USA and the subsequent release of data stored at the centre to the US authorities is inadmissible due to the lack of a corresponding legal basis and on account of its illegality under German law and EC data protection law. In particular, it is pointed out that the USA does not possess an adequate level of data protection pursuant to Art. 25 (1) and (2) of the EC Data Protection Directive. Legal responsibility for the transfer of data to the USA is attributed both to SWIFT and to the banks which avail themselves of SWIFT's services. The banks have been called upon to propose measures as a case of urgency via which the transfer of data to the USA could either be prevented in the SWIFT process or transferred data records could at least be safeguarded adequately to rule out future access by American authorities. Irrespective of such measures, the banks are further called on to inform their clients without delay that when cross-border payment orders are forwarded the data are also transferred to a SWIFT data-processing centre based in the USA.

The current situation also necessitates a clarification of the supervisory structures for SWIFT, which are currently the responsibility of the central banks. In this context, it has to be made clear in particular that the implementation of data protection regulations falls within the scope of these supervisory duties, notwithstanding the powers of national data protection authorities. Furthermore it has to be made sure that the competent authorities are duly and timely notified when necessary in accordance with the relevant regulations. All financial institutions in the EU, including the central banks, which use the SWIFTNet FIN service are to ensure in accordance with Art. 10 and 11 of Directive 95/46/EC that they inform their clients adequately as to the processing of their data and their respective rights. In this context, clients must also be informed that the US authorities are able to access their data. The data protection supervisory authorities will enforce this obligation to provide information for all financial institutions throughout Europe. Beyond this, the financial institutions and central banks should develop technical alternatives to the current procedures, in order to ensure a system for the transfer of payments which is in line with the principles embodied in the Directive.

Figure on 9.4

**The way how SWIFT works**

## 9.5 Warning and information system of the insurance industry – Uniwagnis

*Warning and information systems must be designed in compliance with data protection requirements. The Uniwagnis system employed by the insurance industry does not meet these requirements.*

In assessing an application for an insurance policy or a claim, it may be necessary to obtain information from other insurance agencies or to pass on data to other insurers in order to appraise risks, to clarify the facts relating to a claim or to prevent insurance fraud. To this end, the German insurance sector has developed a warning and information system (Uniwagnis) for various lines of insurance, via which information on policy holders can be exchanged. The policy holder's consent to the use of this system is obtained on the policy proposal form. The warning and information system is operated by the general association of the German insurance industry (GDV) on behalf of the affiliated insurance companies (cf. box on no. 9.5).

When launching the system in 1996, the data protection supervisory authorities considered Uniwagnis and the general declaration of consent given by policy holders at the time of concluding the contract as non-critical in terms of data protection requirements. Now, however, it must be assumed that the consent clause in place to date is no longer in compliance with pertinent law, as the amendment to the Federal Data Protection Act in 2001

requires an adequately specific declaration which meets the conditions determining the effectiveness of such consent as defined in Section 4a para. 1 and 3 of the Federal Data Protection Act. It is not apparent from the clause how extensive the reporting and passing-on of personal data is in the context of the warning and information system, what consequences this may have and when and how reporting takes place. There is an urgent need for policy holders to be informed in greater detail as to the purposes of the system. In this connection, I also refer to the Federal Constitutional Court's decision of 23 October 2006 (cf. 9.6 below).

Notwithstanding the question of the validity of consent, the Uniwagnis system is a source of concern to the data protection supervisory authorities with regard to fundamental aspects of data protection. These concerns relate, among other things, to the lack of transparency and the inadequate scope for monitoring data exchange between the participating insurance agencies when inquiries lead to hits. It is not stipulated, for example, how an inquiring party's justified interest in a piece of information is to be verified or how the exchange of information between the participating insurance companies is to be logged and/or documented when inquiries lead to hits. While the data which are regarded as relevant are noted in the records on the cases concerned, no standard rules exist. The GDV has announced that it intends to remedy this situation by drawing up a so-called compliance guideline.

A particularly problematic aspect from a data protection perspective is the onward transfer of encoded data to all insurance companies, as this entails passing on data which can be related to individuals in a manner which enables the recipients to build up stocks of such data. Other problematic areas are the reporting criteria stipulated by the insurance industry and the lack of opportunity for data subjects to assert their right to the erasure or correction of data because they are not informed when their data are reported to the system. The collection of data on third parties (e.g. accident victims, witnesses, experts) into the system without notification of these data subjects is a further problematic aspect. This is to be regarded as particularly critical, as these third parties have not consented to their personal data being entered in the Uniwagnis system and Sections 28, 29 of the Federal Data Protection Act cannot be cited to justify the transfer of such data because an erosion of the data subjects' legitimate interests is to be assumed when their data are entered in the system without prior notification.

Divergent views prevail between the insurance industry and the data protection supervisory authorities on the legal assessment of Uniwagnis. Against this background, the Düsseldorf group of data protection supervisory authorities has embarked with the GDV on a comprehensive review of data processing in the Uniwagnis system for the private sector, in order to establish a broad basis for further legal evaluation within the supervisory tasks of these authorities. No results were available at the time of going to press.

I will continue to urge for the information and warning system to be organised in a manner which is in compliance with data protection requirements.

Box on section 9.5

#### **How Uniwagnis works:**

In case of claims and payments, the individual insurance companies enter data into the warning and information system according to defined reporting criteria. These criteria are for the most part unknown to the public, in order to prevent policy holders from abusing such knowledge for fraudulent ends. On a separate basis according to the respective lines of insurance, the general association of the German insurance industry (GDV) collects and encrypts data of the policy holder which are communicated by the insurance companies by means of a phonetic structured code method using the UNIWAGNIS I software. This method involves converting phonetically similar sounds into the same numerical sequence. The code consists of several digits, of which five are allocated for the surname, two for the post code, six for the date of birth and one for gender. As a result of the encryption process, the data records of different individuals may be allocated the same code. Individual items of data relating to specific individuals cannot be read out of the database without further ado.

The GDV transfers the encoded data to the affiliated insurance companies via data carrier at least once a month. These companies employ the UNIWAGNIS II software, which also converts the search data into a structured code, to search and read data in the database. In the case of a claim or when an application for an insurance policy is submitted, the insurance company concerned enters the policy holder's or applicant's identification data in the system to search for a match. In case of a match, the inquiring company is informed of the name of the reporting company, in order to contact it and to clarify whether the identity of the phonetic structured code matches the identity of an actual person and whether the data record matches the reason for the inquiry. This is necessary because the same code may be allocated to several different persons. Contact generally takes place by telephone.

### **9.6 Federal Constitutional Court stops insurance companies obtaining consent by way of declarations on standard forms**

*The Federal Constitutional Court has established that general declarations of consent as part of standard forms pertaining to insurance policies constitute a substantial erosion of the data subject's interest in effective self-protection to prevent the abuse of personal data.*

I have long (cf. 20th Annual Report, no. 17.1.9) criticised the outdated general standard declaration which has been used by insurance companies for over 15 years now. In these cases policy holders consent, on taking out an insurance policy, to the collection of sensitive health data which are subject to medical confidentiality at any time in the future. Such indefinite and non-specific "carte blanche" arrangements do not meet the requirements pertaining to informed consent pursuant to the Federal Data Protection Act. The insurance companies are thus required to obtain a separate declaration releasing the medical practitioners concerned from their duty to maintain confidentiality in each individual instance.



This is the only way of providing policy holders with an overview of which of their health data are passed on and when. Regrettably, efforts by the data protection supervisory authorities to attain consensus with the GDV on a new consent clause in compliance with the statutory requirements have thus far been to no avail. At present, the continuing lack of agreement means that, in transferring patients' data to insurance companies on the basis of a blanket declaration of release from the duty to maintain confidentiality, doctors run the risk of breaching their duty of confidentiality pursuant to Section 203 of the German Criminal Code. At my initiative, a provision regulating the collection of health data by the private health insurance funds has thus been adopted into a draft bill on reform of the law on insurance policies (Section 213 of the act to harmonise the Insurance Contract Act with EU legislation – Bundestag document 16/3945).

In its decision of 23 October 2006 (1 BvR 2027/02), the Federal Constitutional Court censured a general declaration of release from the duty to maintain confidentiality in insurance policies as an infringement of the right to determine the use of one's personal data. In the decision it is stated that a declaration which is incorporated into a standard form, and which in some instances is worded in very general terms, constitutes a substantial erosion of the data subject's interest in effective self-protection to prevent the abuse of his or her personal data.

It is asserted that the broad terms in which the declaration is worded mean that it is not foreseeable what items of information may be obtained by whom, thus depriving the data subject of the possibility of monitoring the protection of his or her interests in keeping their personal data confidential.

The Court further referred to a responsibility on the part of the state to ensure and provide the legal basis for effective self-protection in the area of personal data, in the context of the general right to privacy.

The principles set out by the Federal Constitutional Court apply not only to the declaration of release from the duty to maintain confidentiality, however, but must receive due consideration with regard to all declarations of consent to the collection, processing and utilisation of personal data which require to be submitted when taking out a policy. I hope that the insurance sector will finally take the Federal Constitutional Court's decision as an incentive to adapt the outdated general consent clause, which has been used in insurance policies since 1994, in line with the given statutory requirements, as the data protection supervisory authorities have demanded repeatedly. The old clause is not in compliance with the provision contained in Section 4a of the Federal Data Protection Act requiring consent to be based on the policy holder's free decision. Furthermore, it does not render sufficiently apparent what the purpose of collecting, processing and using the policy holder's data is and what the possible consequences may be. The use of a standard clause belonging to a standard fact sheet for different types of policy is not in compliance with data protection law. The fact sheet

contains information on all possible forms of data processing, although only certain parts of this information are relevant to the individual policy. As a consequence, the data subject is not informed with sufficient clarity as to the purpose of collecting, processing and using his or her data.

Notwithstanding the need to amend the consent clause, following the Federal Constitutional Court's explicit appeal to the state bodies I consider it desirable to establish the legal basis for self-protection in matters of personal data and to provide a statutory basis which ensures transparency and is strictly geared to the principle of necessity and proportionality. As the act to reform the law on insurance policies (see above) provides an appropriate means to this end, I have requested the chairpersons of the Committees on Internal and Legal Affairs at the German Bundestag to take account of these considerations in the impending discussions on the draft bill.

The decision also has consequences for other sectors in which personal data are collected and processed on the basis of declarations of consent. Declarations of consent are only valid when the data subjects have a clear understanding of the ramifications involved and are able to decide specifically to whom data is to be available for which purposes. The question as to whether declarations submitted on standard forms meet these requirements must be verified with due care in each instance.

## **10 Telecommunications and teleservices**

### **10.1 An error of judgement in Brussels – The directive on the retention of telecommunications data**

*The Directive on the retention of data entered into force in May 2006. It must be implemented by 15 September 2007.*

Following the “fastest ever legislative process in the history of the EU” – according to MEP Alexander Alvaro, rapporteur of the responsible Committee on Civil Liberties, Justice and Home Affairs – the European Directive introducing the Europe-wide retention of telecommunications data entered into force in May 2006. This Directive obliges providers of telecommunications and internet services to retain an extensive scope of telephone and internet data for the law enforcement agencies, without any concrete suspicion or indications of an impending threat. The Directive is to be implemented into national law by 15 September 2007; an extended deadline of 15 March 2009 applies for the area of internet access, e-mail and VoIP services.

The retention of data entails a substantial encroachment on the privacy and confidentiality of the communications of innocent citizens. It affects particularly sensitive information which falls within the protective ambit of the privacy of telecommunications. Consequently, fundamental concerns and criticism have been voiced in the course of the legislative process by data protection officials and civil rights activists, as well as providers of telecommunications services.

From the point of view of data protection, the most important requirements can be summarised as follows:

- The retention period must be based on the current maximum period for billing purposes, i.e. under German law six months (Section 97 para 3, sentence 3 of the Telecommunications Act). The Directive stipulates this period of six months as the minimum retention period. Under the terms of the Directive, EU Member States can provide in their national legislation for the retention of data up to a maximum period of 2 years
- The purpose of the retention of data in combating terrorism and serious crime must be clearly defined and – as stipulated by the Directive – restricted to these areas.
- The stored data may only be made available to state law enforcement agencies. No access to the data must be granted to private third parties or other state bodies.
- The types of data covered by the retention obligation must be stipulated and narrowly defined.
- As a general principle, a judge should always decide on the release of data.
- The data must not be used by the providers of telecommunications and internet services or by any other bodies for any other purposes, such as economic aims.
- The development of data pools which might serve purposes other than those stipulated is to be avoided. To this end, the retained data should be processed in separate systems. Technical and organisational measures must be provided in this connection to ensure data security.
- The possibility of anonymous e-mail communication must continue to be ensured. To this end, the scope of retained data must not include the user's name, address, date of birth or e-mail address.

In response to an application by Ireland and Slovakia, the European Court of Justice is currently examining whether the retention of data can actually be introduced on the selected statutory basis. Should the European Court of Justice decide as it has done on the question of the legal basis pertaining to the transfer of data on airline passengers to the USA, i.e. “to quash” the Directive, despite the failure of the first attempt back in 2004 due to a lack of unanimity the “old” approach will probably be tried again in an attempt to push through the retention of data via a framework decision.

If the European Court of Justice does not rule that the Directive is in breach of European law, the Federal Republic of Germany will be obliged to implement the Directive. In this connection the Federal Ministry of Justice submitted a draft bill for an “Act to reform phone tapping and other covert investigative measures and to implement Directive 2006/24/EC” in November 2006 (see also no. 6.1). This omnibus bill is also intended to prescribe data retention in the Telecommunications Act. Unfortunately, my call for providers to be obliged to store the data which are retained for prosecution purposes separately from the data which are required for their own business purposes, e.g. for the provision of services and attendant billing, has fallen on deaf ears so far. Neither is there any provision to restrict the purposes of use to the prosecution of terrorism and serious criminal offences. Quite the contrary – the very vague wording “mittels Telekommunikation begangene Straftaten” (“criminal offences committed by means of telecommunications”) goes far beyond this scope of application and is not offset sufficiently by a supplementary clause requiring the weighing-up of general and private interests. With regard to the retention period, the minimum period of six months has been adopted from the Directive.

The further course of development remains to be seen. In a few months’ time, the Federal Constitutional Court is likely to have to consider the question of whether the retention of data is reconcilable with the Basic Law, as civil rights organisations have announced that they intend to lodge constitutional complaints.

## **12 Transport**

*The use of electronic systems in road traffic must not result in a “Big Brother” scenario for motorists.*

We live in a mobile society. There are over 54 million registered motor vehicles on our roads, including 45 million passenger cars and 2.5 million lorries. Many millions of foreign vehicles must be added to this figure. Most vehicles are used on a daily or almost daily basis – for the journey to work, to the kindergarten, to the doctor or to transport goods. The total mileage clocked up each year runs into the billions.

At the same time, the technical possibilities for locating vehicles and for recording and evaluating the distances they travel have improved considerably in recent years. Navigation

systems make it easier to reach one's destination more quickly. Locating facilities have been fitted in some vehicles, to enable them to be tracked down in the event of theft. Locating systems are also being used to an increasing extent to manage fleets of vehicles. A wealth of electronic "helpers" are now installed in virtually every new vehicle as standard, in order to assist the driver and to correct driving errors automatically. To this end, they have to evaluate certain driving parameters on a continuous basis – speed, brake function, cornering behaviour, fuel consumption. The on-board computer indicates when there is a malfunction and when the vehicle is due for a service. The combination of different technologies, satellite location (GPS, soon to be superseded by the even more accurate Galileo system), sensor systems and radio and mobile telephone technology (GPS, UMTS) makes a host of new services possible which were inconceivable only a few years ago. These new applications include the motorway toll system for heavy lorries which went into operation at the beginning of 2005.

There is a downside to all these useful developments in the field of traffic telematics, however. The new technologies have the potential to monitor and record motorists' every move and to match the obtained data with other comprehensive data bases, such as telecommunications call data, government databases or customer profiles. Various areas of application are examined in detail below, from the motorway toll system for lorries to systems which are intended to enhance traffic safety (accident data recorders and eCall).

## **12.1 Lorry toll**

Since the beginning of 2005, Toll Collect GmbH has been charged by the Federal Office for Goods Transport (BAG) with collecting toll charges for heavy lorries with a laden weight of over 12 t, on the basis of the Motorway Toll Act (ABMG). Two types of movement data are generated by the toll collection system: Journey-related data (Section 4 para. 2 ABMG), e.g. route, location and time, and control-related data (Section 7 para. 2 ABMG), e.g. photograph of vehicle, name of person. Processing and use of the toll data are permissible solely for the purposes of the Motorway Toll Act. Consequently, the investigating authorities have no access to any journey-related data which are collected by the toll system.

The scope of data collected in connection with the motorway toll system and the use of these data must also be considered when discussing the possibility of expanding the toll system to other vehicles – an option which is continually being considered. The wholesale transfer to passenger cars of the system which is currently limited to heavy lorries, in which a vast scope of data is recorded on every mile travelled, would be quite unacceptable in my view. Rather, timely consideration needs to be given to alternatives which will not result in the blanket surveillance of all vehicle movements.

### **Is it permissible to use toll data in combating crime?**

*The Federal Government is seeking to relax the restrictions on the use of toll data in the Motorway Toll Act.*

Long before the introduction of the lorry toll charge, the question as to whether such systems might erode data protection was a talking point. The debate centred on how a toll system could be designed in line with data protection needs. A resolution adopted at the Conference of Commissioners for Data Protection of the Federation and the Länder on 9 March 1995 states:

“The introduction of such traffic telematics systems harbours a risk of personal data concerning the whereabouts of millions of motorists being collected and processed. This would enable the generation of precise movement profiles. The technical basis would then be in place to enable systems operators and others to trace who travelled when and where. Such collections of data would be unacceptable from a data protection perspective, because the basic right to the free development of personality also includes the right to the greatest possible freedom of unobserved movement. Against this background it is particularly important to design electronic toll systems in such a way that they conform with the requirements of data protection. Other systems, such as the vignette system, are to be considered as well in the pending decisions.”

In introducing the motorway toll for heavy lorries, the legislature is known to have opted for a system which gives rise to large volumes of individualised data both for the operator of the toll system and for the Federal Office for Goods Transport (see box on no. 12.1). With due consideration to the data protection risks associated with the storage of these data, Section 2 para. 2 and Section 7 para. 2 of the Motorway Toll Act restrict the use of these data to limited purposes. After Gummersbach local court (ref.: 10a GS/239/03) approved the use of toll data for the purposes of criminal prosecution, this restriction of use for the data was further reinforced by a clarification of the legal situation on 2 December 2004 (cf. 20th Annual Report, no. 22.1.2).

This was far from the end of the debate on the use of toll data, however. Following various serious crimes in which heavy lorries and/or their drivers were involved, the question was raised in parliamentary circles as to the extent to which the strict restriction on the use of the toll data was actually appropriate. In the ensuing debate I referred to numerous examples which show how relaxing the restriction on the use of data has ultimately led to very far-reaching opportunities for use. At the same time I have not rejected the political demands point blank, rather urging a careful assessment of the proportionality situation. I am first of all concerned whether the toll data are at all appropriate for prosecution purposes. Should this be confirmed, I would only consider use of the data for certain very serious crimes acceptable,

such as capital offences. It would also have to be ensured that such access could only take place after obtaining a court order. It would further have to be safeguarded that only data which are closely linked to the offence in terms of time and place are used – rather than involving large numbers of innocent persons, as applies in the case of computer-aided profiling and search. There must be no broadening of the scope of data which has been collected to date and no extension of the storage period. If the operator of the toll system were required to retain data which it does not require itself for possible subsequent inquiries by the investigative authorities, this would constitute inadmissible data retention in contravention of our Constitution.

An initial draft ministerial bill from the Federal Ministry of the Interior envisages also permitting the processing and use of toll data for the purposes of prosecuting “serious offences” or “to avert dangers”. I believe this goes too far. I will urge for a solution which upholds the principle of proportionality.

### **Examination of the erasure concept at Toll Collect**

*An examination of Toll Collect’s erasure concept has confirmed that it meets the statutory data protection requirements.*

Around one year after the launch of the motorway toll, I carried out an assessment of data protection management at Toll Collect. The Motorway Toll Act requires Toll Collect to immediately erase the stored journey-related data when no claims for the reimbursement of toll charges are filed in accordance with the specified deadline. As part of the erasure concept which it has developed, Toll Collect carries out internal audits to verify that the system is functioning in compliance with data protection requirements. Toll Collect demonstrated to me how such an audit is carried out by reference to the example of the ÜWS monitoring system which is employed to monitor the company’s own systems and to carry out the long-term detection of potential abuse by those liable to pay the toll charge. This was intended to confirm that the erasure and anonymisation rules resulting from the system’s erasure concept actually take effect in the required manner. To my satisfaction I was able to ascertain that the requirements for the erasure of data pursuant to Section 9 of the Motorway Toll Act are correctly implemented.

### **Check on the handling of toll data at the BAG**

*One aspect covered during an inspection visit to the Federal Office for Goods Transport (BAG) was the Office’s statutory supervisory duty with regard to Toll Collect in the field of data protection.*

A recent inspection visit to the Federal Office for Goods Transport (BAG) centred on establishing how the BAG meets its supervisory duties with regard to Toll Collect in the field

of data protection and how it handles personal data. Section 7 of the Motorway Toll Act assigns the BAG responsibility for monitoring implementation of the toll process. To this end, Toll Collect's internal ÜWS system supplies data to various databases of the BAG on a daily basis. These data serve on the one hand to monitor compliance with the operating agreement and data protection requirements by Toll Collect, while on the other hand the BAG also uses these data in discharging its duties arising from the Motorway Toll Act. The BAG is responsible for ensuring compliance with the erasure deadlines stipulated in the Motorway Toll Act. A conclusive assessment of the erasure concept was not possible at the time of my visit, as the deadline had yet to expire for the vast majority of the data. Where the deadline for the erasure of data had already been reached, I was able to verify that erasure had duly been carried out.

My inspection of the data-processing center revealed that the BAG produces back-ups of its data which are kept for an unlimited period. This is critical from the point of view of data protection, as these back-ups contain data which should have been erased in accordance with the provisions of the Motorway Toll Act. The BAG has undertaken to draw up an appropriate erasure concept.

### **Deployment of video surveillance to verify compliance with the operating agreement**

*Video surveillance provides no grounds for objection with regard to data protection requirements, as no personal data are collected.*

The BAG monitors whether Toll Collect performs the services agreed in the operating agreement (cf. 20th Annual Report, no. 22.1.4). Measures employed to this end include video surveillance at the tolling bridges in order to verify their correct functioning. The BAG deploys video cameras which record the flow of traffic in one direction – i.e. both those vehicles liable to toll charges and those to which no toll applies – for around four hours. The obtained data are subsequently compared with Toll Collect's data. I initially had reservations as to the acceptability in terms of data protection of recording vehicles which are not liable to toll charges, as it is not permissible to record passenger cars under the Motorway Toll Act. I thus proposed deploying the video cameras in such a manner that the registration numbers of the passenger cars could not be identified, thus avoiding any collection of personal data. In the interests of maximum transparency, I also recommended to the BAG that it publicise the fact that it carries out these verification measures and explain their purpose at its internet portal.

I have since examined the BAG's video surveillance measures at the tolling bridges and established that my proposals have been implemented. The statutory data protection requirements are met in the course of subsequent evaluation of the measurements at the BAG, which involves comparing the video recordings of the traffic flows with the corresponding images recorded by the overview camera on the tolling bridge.



Box on section 12.1

**Data which are collected and stored in connection with the lorry toll charge:**

- the amount of the paid toll charge,
- the route for which the toll was paid,
- the time and place at which the toll was paid,
- in the case of payment of the toll prior to using federal motorways subject to the toll charge, the period during which use of the motorways is permissible and the reference number,
- registration number of the vehicle or combination of vehicles,
- the characteristics of the vehicle or combination of vehicles determining the level of the toll charge.

## 12.2 eCall

*As part of the so-called “eSafety Initiative” launched together with the corresponding branches of industry in the spring of 2002 with the aim of improving traffic safety in Europe, the EU Commission is pushing for automatic emergency call devices (In-Vehicle eCall) to be fitted in new motor vehicles as standard.*

The introduction of In-Vehicle eCall (eCall) has a high level of priority in the EU Commission’s efforts to achieve a sustained improvement in traffic safety in Europe. As of September 2010, the Commission envisages all new vehicles being equipped as standard with a device which will initiate an emergency call to the pan-European emergency number, 112, in the event of an accident. In this way it is intended to relay all the data required for fast help to the nearest emergency call station, in particular the location of the vehicle and the time of the accident (see also box on no. 12.2 and Figure 9). This is expected to shorten substantially the time which elapses between an accident occurring and the arrival of professional assistance at the scene of the accident, which could result in considerably more lives being saved than has been possible to date. Details such as how the eCall system is to be activated, the possibility of deactivation by the owner of the vehicle and the contents of the minimum data record to be transferred have yet to be finalised.

From the point of view of data protection, the initial question arises as to whether there is actually any sense in making it compulsory to fit such a system. Those who predominantly drive in built-up areas or on well-frequented roads are unlikely ever to find themselves in a situation in which they require such a system. And in remote areas where so-called “dead

zones” without radio reception apply, the eCall system will be of no more use than a mobile telephone. When a system with which personal data are collected is not necessary, the question as to the need for corresponding compulsory requirements naturally arises. I am emphatically in favour of a voluntary solution here. The corresponding systems should furthermore be designed such that drivers largely retain control over the systems installed for their protection. In particular, this entails the driver being able to activate and deactivate the device himself or herself.

At the same time, I do not wish to confront the data subjects with data protection requirements against their will. Anyone wishing to use such a device in their car should feel free to do so. They should then ensure that the resultant data are protected, however. I consider it equally incumbent on the manufacturers and the providers of corresponding services to ensure the necessary framework here. The restriction on the use of the emergency call system for its intended purpose only must also be ensured, i.e. each module must neither transmit nor be ready to receive data up to the time of an accident and must not be checked into the cellular network. Otherwise, it would be possible for third parties to locate the vehicle – also without the data subject’s consent – and movement profiles could be generated for surveillance or advertising purposes, for example. Other applications for the module should only be permissible with the data subject’s consent or by deliberate actions on the part of the data subject (e.g. use of the module as an on-board cellular radio unit).

The so-called Article 29 Working Party of European Data Protection Commissioners has also considered the topic of “eCall”, adopting a corresponding position paper (see no. 3.3. above). I will be following the further course of development of the eCall system together with the European data protection commissioners and working to ensure that due consideration is accorded to data protection issues.

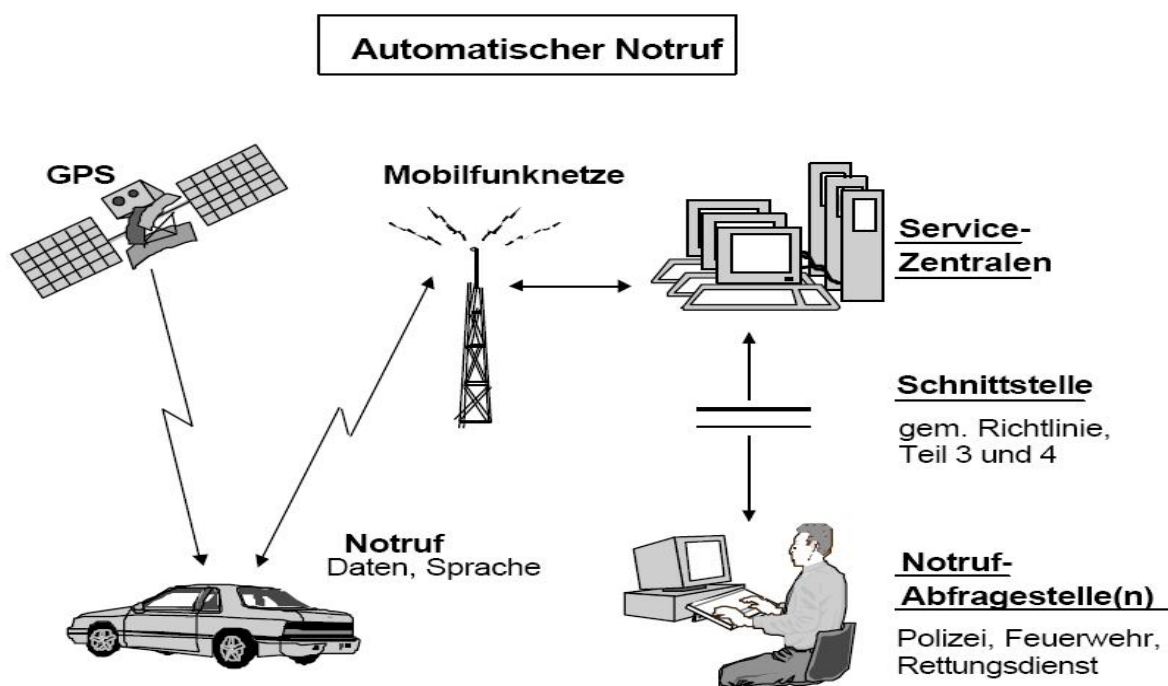
#### Box on section 12.2

##### **How is eCall to work?**

The on-board eCall emergency call function will be activated either manually by the vehicle’s occupants or, after a serious accident, automatically by means of certain sensors in the vehicle. Upon activation, the on-board eCall device dispatches an emergency call with a direct voice and data link to the nearest emergency service – generally the nearest “112” emergency call centre. Via the voice link, the vehicle’s occupants are able to speak to a trained eCall employee. At the same time, a certain minimum scope of data is transferred to the eCall employee taking the call.

This minimum scope of data includes information on the accident, such as time, precise location, vehicle identification and eCall status (specification as to whether the emergency call has been initiated manually or automatically at least) and details of a possible service provider.

Figure on no. 12.2



automatischer Notruf

Mobilfunknetze

Service-Zentralen

Schnittstelle

gem. Richtlinie

Teil 3 und 4

Notruf, Daten, Sprache

Notruf-Abfragestelle

Polizei, Feuerwehr,  
Rettungsdienst

automatic emergency call

mobile networks

service centres

interface pursuant to Directive part 3 and 4

emergency call, data, language

emergency call-inquiry terminal

police, fire-brigade, rescue service

### 12.3 Event data recorder – Big Brother on-board?

*The rapid pace of technological progress offers diverse means of recording and storing data on journeys undertaken by individual vehicles.*

In connection with the above-mentioned EU initiative to improve road safety (see no. 12.2 above), the possible use of journey data recording devices installed in vehicles is also under consideration and is being examined in a broad-ranging research project funded by the Commission. The main focus of the Commission's attention here is on the use of accident

data recorders. These are devices which record journey-related data such as time, axial and lateral acceleration, speed, etc., but only store this information for the period extending from approximately 30 seconds before an accident to 15 seconds after an accident. Scientific studies have shown that the existence of a device tracing the journey induces a more careful driving style in drivers, although this effect diminishes over the course of time. The recording of data also facilitates the considerably more accurate reconstruction of accidents, in view of which the 44th German Verkehrsgerichtstag (an annual conference of traffic experts from the legal, manufacturing and business sectors) at the beginning of 2006 called for accident data recorders to be fitted in vehicles as standard.

Devices employing satellite technology are also under development by industrial manufacturers which will record information on the individual journey and the precise route of the journey while also enabling automated communications between the vehicles and other users of the technology. Such devices, comparable to the on-board units deployed in the motorway toll system, will enable the generation of individual driving and usage profiles.

I note this ever more widespread use of journey data recording devices with some concern, as in conjunction with other technical surveillance measures for road traffic they are clearly conducive to creating a “big brother” scenario on our roads. Consequently, any obligation to install and use these devices must be defined in narrow terms. In this connection I could conceive of an accident data recorder whose recorded data is limited to the events relating directly to an accident. As a general principle, such devices should be installed on a voluntary basis. Only for lorries and buses I would consider the compulsory fitting of accident data recorders reasonable.

From a data protection perspective, the technical design of such journey data recording systems should ensure from the outset that the collection of data in a form which can be linked to specific individuals is ruled out or kept to an absolute minimum and that no central storage is carried out. Experience shows that central databases always arouse a desire to use the collected data for other purposes as well.

## **12.4 Pay as You Drive – Know where You Go**

*Motor vehicle insurers see journey data recording devices as a means of offering “tailor-made” insurance tariffs.*

Insurance companies are testing the use of journey data recording devices with an aim of offering tariffs tailored precisely to individual vehicle usage and the attendant insurance risk – so-called “pay-as-you-drive” tariffs. To this end, the on-board device will record first and foremost the time of day and the covered mileage. Consideration is also being given to the

idea of addressing certain categories of drivers, such as young drivers who are particularly at risk of being involved in accidents (18 to 24 age group), and preventing them from committing traffic offences by means of warnings emitted by the device when speed limits are exceeded, for example, also taking such traffic offences into account when calculating premiums.

For the purposes of data protection it must be ensured that such insurance policies are taken out on a voluntary basis. Equally, the manner in which insurance companies design their tariff systems must not impose any disproportionate economic constraints.

## **15 Deutscher Bundestag – Federal Parliament**

### **15.1 Online facility “Public petitions”**

*Since 1 September 2005 it has been possible to post certain petitions on the Internet for the purposes of public discussion. It is possible to sign such petitions online, provided that they have been accepted as public petitions by the Petitions Committee.*

The two-year pilot project enabling members of the public to sign petitions on the Internet (so-called “public petition”) is based on a system which has been in successful use by the Scottish Regional Parliament since 2001. With this new, interactive online discussion forum, the Petitions Committee of the German Bundestag aims to enable an intensification of communications among citizens and between citizens and the Bundestag.

“Public petitions” are only posted on the Internet with the consent of the petitioner concerned, duly observing the right of privacy. The request or complaint must fall within the German Bundestag’s sphere of competence and concern an issue of general interest. The Petitions Committee decides whether a petition is to be posted on the Internet as a public petition on the basis of published procedural principles and a guideline setting out these principles in concrete terms. Anyone can support a petition which is published online or submit comments on it in a discussion forum. The course of public petition procedures can also be followed on the website of the German Bundestag ([www.bundestag.de/Petitionen](http://www.bundestag.de/Petitionen)).

I have since received numerous complaints concerning this new online facility. The complaint regarding a petition that, contrary to the petitioner’s wishes, was not accepted as a public petition did not hold water, however, as there is specifically no legal entitlement to acceptance of a petition as a public petition. Where several petitioners apply on the same day for a petition to be posted as a public petition on the same topic, acceptance as a public petition may be refused on grounds of equal treatment. In such cases, however, the Petitions Committee could consider appointing one main petitioner – by drawing lots, for example – and treating the other petitioners as supporters.

Other complaints by persons signing public petitions relate to the fact that the names of those signing the petition can be recorded by search engines. It is claimed that the German Bundestag has a duty to ensure that the lists of persons participating in discussions and signing petitions are blocked for search engines. By its very nature, a public petition posted on the Internet is generally accessible and can also be located by search engines. Furthermore,

petitioners, persons signing petitions and those participating in discussions are informed on the Internet platform that participation in a public petition entails the publication of various items of data, including their own name. I nevertheless welcome the current plans of the Petitions Committee of the German Bundestag to evolve mechanisms that will prevent the names of persons participating in discussions and signing public petitions from being captured by search engines.