Annual Activity Report 2009/2010
of the Federal Commissioner for Data Protection and Freedom of Information

(Exerpt)

1 MODERNIZING DATA PROTECTION LAW 5

1.1 Modernizing data protection law: A never-ending story? 5

1.2 Key issues at the Data Protection Conference: The course is set 6

1.3 Data protection via technology and organization 8

1.4 The public discussion has begun 10

1.5 What is next for IT and data protection? 11

1.6 Is there a digital eraser? 13

2 THE LEGAL FRAMEWORK FOR DATA PROTECTION 15

2.1 Lessons from Luxembourg: Germany's data supervision is not independent 15

3 ELECTRONIC IDENTITY 19

3.1 Electronic identity verification and privacy-by-design strategies 20

3.2 The new identity card 22

3.3 De-Mail: The secure way to communicate in future? 24

3.5 Biometrics for border checks 26

4 THE INTERNET 28

4.1 Locating the individual: Geodata and privacy rights 28

4.1.1 My home on the Internet: Google's Street View and other services 29

4.1.2 Gathering WLAN data 32

4.1.3 Self-regulation or legislation? A new regulatory framework for geodata services 33

4.1.4 Geodata in the public sector 37

4.2 The right to object to the publication of personal data on the Internet 39

4.3 Unnoticed: Web analysis programs in the service of website operators 40
4.3.2 Disagreement over IP addresses continues 42

4.4 A long process comes to an end: The EU telecommunications directives have been adopted 43

4.5 In good hands? In the clutches of social networks 46

4.6 And now: What has happened to the Act to Impede Access to Child Pornography in Communication Networks? 47

4.7 ACTA: No data retention for possible future use in the private sector 49

4.8 Identifying IP addresses to fight copyright violations 50

4.9 The Joint Internet Surveillance Centre of the security authorities 51

4.11 Improving international cooperation on data protection 52

5 TECHNOLOGICAL DATA PROTECTION 54

5.1 Smart metering: The intelligent electricity meter 57

5.3 Privacy framework/technical standardization 60

5.4 Collected once, stored forever? Problems with data deletion 62

5.6 Cloud computing: Data protection in the cloud? 63

5.8 Electronic engine control units: Cars as computers on wheels 66

5.9 RFID PIA at European level 67

6 TELECOMMUNICATIONS AND POSTAL SERVICES 69

6.1 Data retention: Quo vadis? 69

6.2 They know where you are: The growth of location services 75

6.5 Deep Packet Inspection: Are operators allowed to inspect communication content? 79

6.7 The underestimated risk of interception 81

6.8 The E-Postbrief is on its way. Will it arrive safely? 83

6.9 Due diligence requirements of telecommunications companies vis-à-vis their customers 86

6.10 Re-assignment of e-mail addresses 87

7 INTERNAL SECURITY 87

7.1 Federal security architecture 87

7.1.2 The counter-terrorism database of the federal intelligence services 87

7.1.3 Logging conducted by the security authorities 88

7.1.7 Police investigation using social media 89

7.2 Federal Criminal Police Office 90

7.2.1 Very late: A statutory instrument on the types of data which the BKA as central agency may store 90

7.2.2 Politically motivated crime: The BKA's IGAST database 92

7.3 Federal Police 94

7.3.1 Full-body scanners at German airports: Progress and problems 94

7.3.2 Biometric border checks at airports: Sorting airline passengers into risk categories? 96

7.3.3 Federal Police introduce electronic criminal records 97

7.4 Preventive telecommunications surveillance and telecommunications interception at the source 98

7.5.1 Should the federal and *Länder* domestic intelligence agencies be allowed to set up a comprehensive information pool? 100

7.5.2 Problems with the right to information from the domestic intelligence agencies 103

7.6 Intelligence services 104

7.6.1 Data processing conducted by the Federal Intelligence Service 104

8.1.1 The 2011 census 105

8.2 Law on foreigners 107

8.2.1 Central Register of Foreigners: Time to provide better protection for the data of EU citizens! 107

8.2.2 The electronic residence title: A document in credit-card format, with fingerprints 108

9 FINANCIAL MATTERS 110

9.1 CD-ROMs of data on tax cheats: Data protection should not go out the window because of government budget deficits! 110

9.2 The power of tax identification numbers 112

9.3 Introducing the electronic wage tax card 113

9.7 Sharing tax-related information with other countries 117

10 BUSINESS AND TRANSPORT 117

10.1 Binding corporate rules 117

10.8 A Europe-wide motorway toll? Only with good data protection! 118

12 PROTECTION OF EMPLOYEE DATA 119

12.1 Protection of employee data: Good things take time? 119

EUROPE AND INTERNATIONAL AFFAIRS 122

13.1 Treaty of Lisbon brings changes for data protection 122

13.2 Amending the European Data Protection Directive 123

13.3 The Article 29 Data Protection Working Party 124

13.4 Safe Harbour 126

13.5 New developments between Stockholm and Lisbon 129

13.6 Selling out to the U.S. on European financial data? 132

13.7 Checking data against lists of terrorists 135

13.8 A new framework agreement with the U.S. 137

13.9 Airline passenger data 138

13.9.1 New developments in agreements with third countries on airline passenger data 139

13.9.2 Will customs authorities soon have access to passenger data too? 140

13.10 Implementing the "Swedish Initiative" 140

13.11 Europol 141

13.11.1 Europol: Central office for police information-sharing in the EU 141

13.11.2 Complaints from Germany to Europol's Appeals Committee 143

13.12 International organizations 144

13.13 European Privacy and Data Protection Commissioners' Conference 145

13.14 International Conference of Data Protection and Privacy Commissioners 145

15 IMPORTANT ITEMS FROM PAST ANNUAL REPORTS 146

1 Modernizing data protection law

1.1 Modernizing data protection law: A never-ending story?

Now that isolated improvements have been made to data protection law, a general overhaul is urgently needed.

Ten years have passed since the Federal Data Protection Act (BDSG) last underwent a major revision: In 1998, the governing coalition of Social Democrats and Greens decided to thoroughly revise Germany's data protection law. Instead, however, in 2001 they took only the small step of revising the Act in line with the EU Data Protection Directive, which had entered into force in 1995. Immediately after this amendment, the "second phase" of data protection reform was to be undertaken – at least according to the Federal Ministry of the Interior. To prepare for this fundamental modernization, the Federal Ministry of the Interior had commissioned a comprehensive report, which was completed in autumn 2001 (Roßnagel, Pfitzmann, Garstka, *Modernisierung des Datenschutzrechts* (Modernizing data protection law), 2001). However, no further action has been taken to date, despite changing political majorities and despite the growing urgency of such reform (see the 22nd Annual Report, no. 2.1).

It is generally acknowledged that data protection law urgently requires a general overhaul. The German Bundestag has repeatedly called for such steps, for example in its unanimous resolutions on my 21st Annual Report (see no. 2, Annex 4) and 22nd Annual Report (no. 1, 2, 3, Annex 5).

During the reporting period, new rules were formulated for individual areas where data protection scandals and public debate had revealed a need for action (see nos. 2.2 and 2.3). But the basic structure of data protection law is still awaiting a fundamental revision.

Sometimes one has the impression that the reform backlog in data protection law has grown so large that no one has the heart to take on this enormous task. In view of the growing challenges, however, remaining with the legal status quo would have devastating consequences extending to the gradual erosion of individual privacy.

In order to start moving on the modernization of data protection law, the Conference of Data Protection Commissioners of the Federation and the *Länder* established a working group, which under my direction drafted specific recommendations for data protection reform. In March 2010, the Data Protection Conference adopted the paper "Ein modernes Datenschutzrecht für das 21. Jahrhundert" (Modern data protection law for the 21st century) (see Annex 6) and presented it to the public.

1.2 Key issues at the Data Protection Conference: The course is set

The outline paper of the Data Protection Conference is intended to set the parameters for the reform discussion.

The paper outlines the central challenges to data protection, analyses the shortcomings of the current legal framework and draws conclusions in the form of specific recommendations for future regulation.

For the overall design of data protection law, the paper recommends passing legislation in which central, generally applicable aims of protection defining a binding minimum standard would be anchored. These aims should provide the foundation for all data protection regulation and measures for public- and private-sector bodies. Based on this foundation, central principles, in particular necessity, restrictions on use and the ban on secretly creating profiles, should be anchored and enforced with appropriate sanctions.

The handling of personal data should always be open and transparent; the principle of data reduction and data economy should be binding and should be more effectively enforceable. The paper also recommends that, for data processing in divided systems (such as cloud computing) or involving multiple bodies (as in the case of central databases jointly run by multiple bodies), responsibilities under data protection law should be defined in a way that makes it easier to comply with data protection law and to monitor such compliance.

To ensure technical and organizational data protection and data security, in place of specific measures fixed to a certain technical environment, general and binding protection goals should be set by law. Doing so would create a technology-neutral and flexible approach capable of doing justice to the constitutional right to determine the use of one's own data and the right to confidentiality and integrity of information

technology systems even under changing technological or organizational framework conditions (see below).

Data protection is not an end in itself; it is focused on the individual, whose basic rights are affected by the processing of his or her personal data. Data processing therefore needs to be more transparent. Data subjects must be able to exercise their rights to information, correction and deletion easily and using electronic media. Developers and users of IT systems should be required by law to provide and apply technology which is conducive to data protection ("privacy by design"; see no. 3.1). Data subjects, who are increasingly becoming active participants in IT processes in which they use their own and others' personal data, should have access to IT products and services with preferences set to ensure the highest level of data protection ("privacy by default").

Data protection law must be capable of dealing with the Internet. In this context, the typically unmonitored use of electronic services plays a key role. It is necessary to create the conditions enabling data subjects to adequately exercise their rights also on the Internet. Just as the Internet is global, minimum legal standards of data protection must apply and be enforceable globally.

Legal mandates for a high and binding level of data protection continue to be important. However, we must also increase incentives so that controllers will view data protection as being in their own interest, for example by means of data protection audits, that is, independent inspections to certify the data protection aspects of products and services. Data protection audits whose quality is guaranteed by law could help products which are conducive to data protection be more successful in market competition.

Government data protection oversight and its independence must be strengthened in order to guarantee enforcement of data protection law in practice. For example, the staffing and budgets of the supervisory authorities must be adequate to carry out their growing tasks, and they need effective powers of enforcement. The requirements for independent data protection supervision defined by the European Court of Law in its decision of 9 March 2010 (cf. no. 2.1) must be implemented soon at federal and state level.

Current sanctions in case of violations of data protection law have sometimes proved inadequate. This is why we must make it easier to enforce claims for compensation and to prosecute administrative offences.

Finally, we must make data protection law easier to understand and therefore easier to apply. Due to the many amendments since 1990, some provisions of the Federal Data Protection Act have become so extensive that users – even those with legal training – can hardly understand them. And contradictions, gaps and excessive regulation have arisen in some cases, almost guaranteeing uncertainty and conflict over the interpretation of provisions.

I hope that our recommendations will take the data protection policy discussion on fundamental modernization to a new level and ultimately lead to legislative action. I see it as a positive sign that the German Bundestag has received our paper favourably and has called on the Federal Government to examine ways to implement it (see no. 6, Annex 5). I will of course refer to these recommendations also in the discussion of restructuring the European legal framework (see no. 13.2).

The complete paper is included in this report as Annex 6 and is available on my website.

1.3 Data protection via technology and organization

In the Data Protection Conference recommendations for reform, technological and organizational components play an important role.

Based on Articles 1 and 2 of the Basic Law, the Federal Constitutional Court has defined the right to confidentiality and integrity of information technology systems as a new basic right (Decision of the Federal Constitutional Court on the basic right to confidentiality and integrity of information technology systems, 1 BvR 370/07 of 27 February 2008). As a result, the validity of these two classic aims of protection, which have already found their way into some data protection legislation of the *Länder*, has been confirmed in constitutional law. For this reason, the following conditions should be taken into account when considering the further development of technical and organizational provisions in data protection legislation:

1. Elementary aims of protection should lay the groundwork for systematically deriving additional aims (of protection). The aims of protection should be simple, understandable and practical (see box for no. 1.3).

2. The aims of protection correspond to the elementary aims of protection of IT security (availability, integrity, confidentiality) and partly overlap with these. At the

same time, however, the special perspective of data protection should be brought to bear.

3. The aims of protection must be sustainable over the long term.

4. It should be possible to base application-independent and specific catalogues of data protection measures on the aims of protection, which, like the BSI's IT basic protection catalogue, can be implemented in flexible, practical and software-supported procedures and can serve as catalogues of criteria for data protection audits.

5. The basic aims of protection should be defined independently of specific technology as far as possible, while the measures based on them should take into account the specifications and operating conditions of the various IT systems. This means: The aims of protection remain the same, while the measures must constantly be updated.

6. IT systems should be configured in compliance with and ideally support the basic legal requirements of data protection (data reduction, data economy, restrictions on use, rights of data subjects such as correction and deletion). Concepts such as system data protection and privacy-enhancing technology (PET) take up this idea. Exemplary:
   - deletability must be implementable
   - technical implementation of data subjects' rights (e.g. right to information, correction and deletion)
   - identity management (anonymization and aliasing)
   - revision-proof logging (i.e. not even the system administration can make changes)

7. It must be possible to adequately represent the technical and organizational measures resulting from technological progress and technologies conducive to data protection.

In the interest of preventive system data protection, the technical and organizational measures should be taken even before it is known that personal data are to be processed. Instead, the many options for personalizing anonymous data and the subsequent inclusion of personal data should be taken into account. Precautions to be taken in such cases include those preventing the unauthorized de-anonymization or personalization of data.

Box for no. 1.3

Elementary data protection aims

Availability:	Guaranteeing that personal data and procedures for processing them are available on time and can be applied appropriately.
Confidentiality:	Ruling out the possibility of unauthorized access to personal data and procedures.
Integrity:	Guaranteeing the integrity, attributability and completeness of data from processes used with personal data.
Transparency:	Guaranteeing that the collection, processing and use of personal data can be understood, inspected and evaluated with a reasonable effort.
Restrictions on use:	Guaranteeing that processes used with personal data are organized in such a way that the data cannot be collected, processed or used for any other purpose than that indicated, or that doing so would require excessive effort.
Ability to intervene:	Guaranteeing that processes used with personal data are organized in such a way that data subjects can effectively exercise their rights.

1.4 The public discussion has begun

The outline paper was presented to a broad audience.

In order to present the proposals for reform to those in the field of data protection, and to discuss the key issues with experts, the Conference of Data Protection Commissioners of the Federation and the *Länder* organized a symposium on modernizing data protection law in Berlin on 4 October 2010 (see also no. 14.1).

Two expert presentations focused on basic legal and technological issues.

State Secretary Cornelia Rogall-Grothe of the Federal Ministry of the Interior presented the Federal Government's position. She welcomed the data protection commissioners' specific proposals for improving data protection law presented in their outline paper. The Federal Ministry of the Interior sees the greatest need for action in improving data protection on the Internet. State Secretary Rogall-Grothe stated that in the 17th legislative term, the Federal Ministry of the Interior had increasingly addressed Internet policy issues, to which data protection law certainly belonged. She said that the ministry set a priority on voluntary regulation, for example with regard to a code of conduct for personal geodata (see no. 4.1.3).

Prof. Friedemann Mattern of the Swiss Federal Institute of Technology (ETH) in Zurich explained what technological developments can be expected in the near future, what these will mean for the right to determine the use of one's personal data, and what options information technology offers to manage emerging risks. Prof. Mattern especially focused on mobile technology and the possibility to link location data with additional information about the data subject, saying that the real and the virtual world were becoming ever more strongly linked and that increasingly comprehensive and detailed information about individuals' behaviour was being generated.

A panel discussion with representatives from the world of politics (Jan Philipp Albrecht, MEP), law (Prof. Michael Kloepfer), computer science (Prof. Hannes Federrath), industry (Prof. Dieter Kempf, BITKOM) and data protection supervision (Dr Alexander Dix) provided an opportunity to discuss individual issues in greater detail. In addition to the issues already mentioned, these included the European and international dimensions. For example, it was considered important that the Data Protection Conference recommendations played a role in the debate over restructuring the European legal framework on data protection. Participants agreed that international companies based outside Europe but active in European markets should be more accountable under European data protection law.

1.5 What is next for IT and data protection?

New information technologies continue to be associated with growing risks to privacy. They have entered all areas of life and bring additional potential for monitoring.

Data protection law must be aware of technological developments. That is easier said than done, because forecasting technological developments is extremely imprecise. Formulating general aims of protection (see above) and integrating technical

innovations in data protection law in an abstract and technology-neutral way must keep up with the enormous speed of innovation in the IT sector – a challenging task!

The trend to ever smaller and more powerful IT systems also continued unabated during the reporting period, and networking in IT continues its inexorable progress.

The upgrading and linking of previously separate IT systems, new software strategies and business models create ever more extensive potential for monitoring by government bodies and businesses. It is therefore all the more important to take these risks into account by means of regulations and technological solutions in order to protect individual privacy rights.

This is why fundamental requirements are aimed at data economy, the anonymous use of services/use of an alias, the use of identity management systems conducive to data protection, transparency of all processing and a ban on creating personal profiles without the knowledge and consent of data subjects. In view of the growing importance and rapid development of information and communications technologies, it is essential to improve IT literacy through basic and advanced training in all areas of society.

The following examples are intended to illustrate how IT systems have a growing influence on our private and professional lives and are entering ever more areas of life:

- Social networks
  Today it is child's play to publish personal information and photos on the Internet. Many people exercise far too little caution in entrusting private information – also of third persons – to the Internet without regard for the consequences.

- Ubiquitous computing
  More and more products are equipped with RFID tags (see no. 5.9) which can be read by stationary monitoring units and other "smart" devices at a distance of a few centimetres or metres. In this way, data processing is becoming ubiquitous.

- Geolocation
  The trend towards constantly determining the location of mobile devices (such as smartphones and laptops) via GSM- and WLAN-networks and forwarding this information – in some cases without the user's knowledge – continues unabated. This information can be combined with other sources (such as electronic

telephone and address registries, street view software, entries in social networks) to create movement, behaviour and personality profiles.

- Biometrics
  Methods of biometric recognition today are available not only to government bodies and businesses; they can be used by practically anyone. I find it unsettling when digital photos, such as those taken using smartphones, can be used to identify ordinary people by comparing them with photos published on the Internet or in social networks.

- Cloud computing
  The use of (standardized) services via the Internet, as in the case of cloud computing (see no. 5.6) could revolutionize the entire IT industry and the way we use IT. But “software as a service” should not be allowed to let responsibility for data processing and the ability to supervise it vanish into the cloud.

- Convergence of services and networks
  The integrated use of the Internet, language services and multimedia content multiplies the specific risks through interaction between these services and cumulative effects among service providers.

1.6 Is there a digital eraser?

It should go without saying that personal data can be erased. But this is not the case in practice, especially on the Internet.

One of the basic requirements of data protection is to delete personal data when they are no longer needed for the purpose for which they were collected or when they were collected without authorization. What should therefore go without saying, according to the law and the rulings of the Federal Constitutional Court, leads in practice to major difficulties (see for example no. 5.4).

The question of erasing data on the Internet, which by its nature is oriented towards global dissemination and unlimited use of information once published, remains largely unresolved. The problems start with the providers of online services, which either fail to offer any possibility for deleting information once posted or offer them only in difficult-to-find settings. But even if this function is available and data subjects take advantage of it, it does not always mean their data will indeed be removed. Often the data remain stored and can be analysed later.

In addition, online services often provide technical ways to make personal data available to other providers, which then store the data themselves and are never informed when these data are later deleted.

So effective data protection in the Internet age must aim to teach the Internet how to forget or develop an Internet eraser.

Upon closer examination, however, the problem of removing one's personal information from the Internet easily and permanently becomes almost insoluble. The real-word eraser proves impossible to duplicate in the digital world, as it assumes that data subjects know all the places where their data are published on the Internet and that they truly have control over their own data.

The idea of an expiration date on the Internet – independent of the rules for individual service providers – was recently given initial shape. In a system developed at the University of Saarbrücken (x-pire), the data subject publishes her personal data on the Internet in encrypted form; when other users download the data, they are decrypted. By defining how long the necessary decryption key should remain valid, the data subject determines how long her data can be accessed.

This solution met with some criticism, raising questions as to the trustworthiness of the key administrator or how to prevent downloaded data from being copied and published elsewhere. Nonetheless, I find this contribution helpful in the effort to develop ways to ensure the right of individuals to delete their personal data from the Internet.

Additional approaches are needed to give users as much control as possible over their data.

- The principles of data reduction and data economy must apply at the time the data are collected. Services should be designed to collect and store only those data which are truly necessary. It should be possible to use services under an alias.
- Default settings should be conducive to data protection, ensuring that user-provided content can be accessed only by a group defined by that user. Content should be made available to a general, global Internet audience only at users' explicit wish.

- Providers should be required to make access to the delete function as simple and understandable as possible.
- Publishing personal data of third persons without their knowledge should be regulated and should always be subject to the data subject's consent.
- Online providers should be allowed to make personal data available to third parties (such as software developers and providers of games or other services) only with the explicit consent of the user after explicitly informing her which recipients may access, copy, store and evaluate the data and for which purposes.

Technical and legal solutions for these issues are urgently needed, but they will be effective only if they are internationally accepted and enforceable. For this reason, efforts to improve data protection at the European and global level are extremely important (see no. 13.2).

2 The legal framework for data protection

2.1 Lessons from Luxembourg: Germany's data supervision is not independent

As the European Court of Law ruled on 9 March 2010 (C-518/07), data supervision in Germany's private sector does not satisfy the conditions for complete independence as defined in the EC Data Protection Directive 95/46. The Court's judgement now needs to be rapidly implemented, at both federal and state level.

The European Commission initiated the proceedings (see the 21st Annual Report, no. 2.2), because in its view, the organization of data supervisory authorities for the private sector in Germany violated Art. 28 (1) of the EC Data Protection Directive: The supervisory authorities could not perform their duties with the required "complete independence". This applied not only to those *Länder* in which the supervisory authorities are located in agencies within the internal administration or the interior ministry itself, but also to those *Länder* where the supervision of the private sector was assigned to the *Land* data protection commissioner.

The European Court of Justice largely agreed with this view. Its judgement clearly states that supervisory authorities must be free from all external influence. According to the Court, complete independence means not only freedom from influence by the bodies under their supervision (functional independence); complete independence must be understood in the broad sense: a supervising authority must be free from

any political or institutional influence, for example supervision by other authorities. Even the appearance of such influence must be avoided.

In order to comply with the court's judgement, most of the *Länder* will have to change the organizational status of their supervisory authorities, as these authorities are usually subject to legal supervision or are part of the internal administration and thus even subject to expert supervision. Neither complies with European law. According to the court, administrative supervision must be restricted to ensure that it cannot result in direct or indirect influence on decisions made by the supervisory authority. The judicial independence of members of the federal and state courts of audit could serve as a model.

As a result of this judgement, almost all the *Länder* are working to comply with the requirements defined by the court. Most of the *Länder* in which private-sector supervision is still carried out by agencies of the internal administration are planning to transfer this task to the *Land* data protection commissioners or have already done so.

The 79th Conference of Data Protection Commissioners of the Federation and the *Länder* on 17–18 March 2010 adopted a resolution calling for rapid compliance with the judgement (see box for no. 2.1).

Even though the European Court of Justice judgement formally addresses only the state supervisory authorities for the processing of personal data outside the public sector, it has consequences for supervision in the public sector as well, because the EC Data Protection Directive requirement of complete independence for supervisory authorities is not limited to the private sector. In the public sector it is even more important that the executive should have no influence over the supervisory authorities, since the executive is under their supervision. Thus the standards set by the European Court of Justice apply even more to the public sector.

So my office also needs greater independence, in particular with regard to my legal status. In performing his duties, the Federal Commissioner for Data Protection and Freedom of Information is subject to the legal supervision of the Federal Government. Although legal supervision – unlike expert supervision – cannot exert any direct influence on my decisions, the Federal Government can determine basic issues of interpretation and thus set the direction for how I carry out my duties. This violates European law. Even though no legal supervision has so far been exercised, the possibility of such influence contradicts the complete independence required by

the Directive. Further, it creates precisely that appearance of influence which according to the judgement is to be avoided. And the administrative supervision of the Federal Ministry of the Interior over the staff of the Federal Commissioner for Data Protection and Freedom of Information and his right to hire should be questioned, along with the Federal Ministry of the Interior's right to appoint the senior officer.

Nor do I have the powers of enforcement required under European law with regard to supervising post and telecommunications operators or commercial enterprises under public law: Unlike the data protection commissioners of the *Länder*, I do not have the authority to prohibit the unauthorized processing of personal data, to recall corporate data protection officials who fail to meet legal requirements, or to issue fines. Instead, I must approach the relevant expert supervisory authorities (such as the Federal Network Agency for the post and telecommunications sector) and try to convince them to take action. In the past, there were times I disagreed with these agencies, which are subject to the orders of the ministries.

But even these supervisory authorities do not perform the same duties as the data protection supervisory authorities under Section 38 of the Federal Data Protection Act and, unless explicitly granted additional legal authority, they can take action only in case of violations of specific regulations, such as data protection provisions in the Telecommunications Act (TKG). They are not authorized to impose sanctions for violations of other data protection provisions, such as those in the Federal Data Protection Act. Nor do they have the power to prohibit data processing in case of serious violations or to recall corporate data protection officials. For this reason, the Federal Commissioner for Data Protection and Freedom of Information should be granted authority in these areas, which the *Länder* data protection supervisory authorities have, including the power to prosecute and impose sanctions in case of administrative offences under the Federal Data Protection Act.

However, the Federal Ministry of the Interior has so far seen no need for action, as the court's judgement did not address the legal status of the Federal Commissioner for Data Protection and Freedom of Information.

Furthermore, the autonomous data protection supervision of religious communities and in the administration of public broadcasters should also be examined, as it also lacks complete independence as defined in European law.

Apart from its concrete implementation, the court judgement could serve as an opportunity to re-examine the fragmented system of data protection supervision in Germany. Given the differing jurisdictions of supervisory authorities, it is not always possible to ensure effective and rapid supervision especially in the case of companies active nation-wide, Europe-wide or globally, despite intensive efforts by bodies such as the Düsseldorf Group of supervisory authorities.

Box for no. 2.1

Resolution of the 79th Conference of Data Protection Commissioners of the Federation and the *Länder* of 17–18 March 2010

Effective data protection requires independent monitoring!

In order to enforce citizens' basic right to data protection, independent data protection monitoring is needed. The European Court of Justice found that the supervisory authorities for the monitoring of data processing outside the public sector are not completely independent and that the Federal Republic of Germany has therefore failed to fulfil its obligations under Art. 28 of Directive 95/46/EC (Judgement of 9 March 2010, C-518/07). Not only the fact that many data protection supervisory authorities for the private sector are part of the state interior ministries, but also the government supervision of the supervisory authorities violates European law. Fundamental restructuring of data protection supervision in Germany is advised. The principles of this decision on independence are to be applied to the data protection monitoring of public bodies.

The Conference of Data Protection Commissioners of the Federation and the *Länder* calls on federal and state legislators to restructure data protection supervision as quickly as possible in line with the provisions of Directive 95/46/EC.

In order to ensure the complete independence of the data protection supervisory authorities, the following criteria in particular must be met:

- The supervisory authorities must be able to perform their duties free of all direct and indirect influence from third parties.
- They must not be subject to expert or legal supervision.
- No administrative supervision may lead to indirect or direct influence on decisions made by the data protection authorities.
- They must be free of any influence from bodies under their supervision.

- Independence in performing their duties requires sufficient powers of intervention and enforcement.
- In order to ensure that the data protection supervisory authorities perform their duties independently, they must have the necessary decision-making authority in staffing, budgetary and organizational matters.

3 Electronic identity

“Who am I – and if so, how many?” is the title of the 2010 non-fiction bestseller by Richard D. Precht. One could ask the same question about our identities on the Internet, in government records or in social networks. The amount of personal data held by government and private agencies is constantly growing. It is easy to link various information and create credible, detailed personality profiles of individuals.

Examples of electronic identities are the personal De-Mail address (see no. 3.3), the tax identification number (see no. 9.2) and user names for online shops and social networks.

The individual’s right to determine the use of her personal data is in danger if these and similar data are linked without the necessary legal underpinning. So technologies are needed which allow data subjects themselves to decide which electronic identities are used where. The paper “Ein modernes Datenschutzrecht für das 21. Jahrhundert” (Modern data protection law for the 21st century) adopted by the Conference of Data Protection Commissioners of the Federation and the *Länder* (see no. 1) points out the need for identity management which is conducive to data protection. “Identity management should be based on the anonymous or pseudonymous use of electronic processes and local storage of identifying data, under the greatest possible control by the data subjects.”

With the introduction of the new electronic identity card (see no. 3.2), the issue of identity management assumes even greater importance, as for the first time the government will issue individuals an electronic identity. The card will enable authentication for use with government and private-sector websites as well as the use of different aliases for different applications.

To protect against identity theft and unlawful profiling, it is becoming increasingly important to create a way for individuals to manage their own identities. Such a

system must be easy to use and transparent; from a technological standpoint, standardized interfaces and the possibility of independent review should be required.

3.1 Electronic identity verification and privacy-by-design strategies

In view of rapid technological change, the special requirements of data protection should be considered at the earliest possible stage.

New technological systems often have hidden risks which are difficult to remedy once the basic outline has been set. So it makes more sense to identify and test any problems with data protection during the earliest phases of developing new technologies. This approach is known as “privacy by design” (PbD).

The idea of incorporating technical data protection into IT systems is not entirely new. For example, recital 46 of Directive 95/46/EC states that “appropriate technical and organizational measures [should] be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security”.

Privacy by design is valuable for all kinds of IT systems used for processing personal data. PbD should be a key requirement for all products and services for third parties and individual clients (e.g. WiFi routers, social networks and search engines). Many users have only limited IT skills and are therefore unable to take the necessary security measures themselves in order to protect their own personal data or that of third persons. This is why the default settings for such IT processes should ensure basic data protection (privacy by default).

In addition, providers should also help users protect their personal data better, for example by offering appropriate tools (access controls, encryption, measures for anonymous use).

But PbD does more than just provide security; it also means designing and building systems to minimize the amount of personal data to be processed. Important elements of data economy include separating personal identifying features from content data, using aliases, rendering anonymous and deleting personal data as soon as possible. Good examples of PbD in Germany are the digital health card (eGK) (see no. 3.5), the new identity card (nPA) (see no. 3.3) and the electronic proof of earnings (ELENA) (see no. 3.9).

The basic principle of PbD should be binding for technology developers and manufacturers as well as those who are responsible for the data and for acquiring and operating IT systems. They should be required to provide for technical data protection already in the planning phase of IT processes and systems. Providers of IT systems and services should demonstrate that they have taken all necessary measures to satisfy this requirement.

The growing importance of data protection during the development and operation of IT systems places additional demands on IT specialists. Data protection should therefore be an important part of their training.

Box for no. 3.1

Aims of data protection

Decisions on designing, acquiring and operating a processing system should take the following general aims into account:

Data reduction: Data processing systems should be designed and chosen to collect and use as few personal data as possible.

Control: An IT system should give data subjects effective control over their personal data. Technological means should help with the possibility to agree or reject.

Transparency: Both developers and operators of IT systems must make sure that data subjects are thoroughly informed about how the systems work.

Data confidentiality: IT systems should be designed and secured so that only authorized bodies have access to personal data.

Data quality: Those responsible for data must support data quality using technical means. Relevant data should be accessible for lawful purposes as needed.

Possibility of separation: IT systems which can be used for different purposes or are operated in a multiple-user environment (i.e. virtually linked systems such as data warehouses and cloud computing) must make sure that data and processes used for different tasks or purposes can be securely separated.

3.2 The new identity card

The new identity card is supposed to do more than the old one, but is it also good for data protection?

The new electronic identity card was launched on 1 November 2010.
It is the size of a credit card and, in addition to the “classic” identification function, it can serve as electronic identity verification for e-commerce and e-government functions. This is why, in addition to further security features, the card has a chip, with a secure area for biometric data, the electronic identity verification function and the qualified electronic signature function. The chip contains all the data printed on the card other than height, eye colour and the card holder’s signature.

The draft legislation at first required fingerprints to be stored on the chip, but after criticism from me and others, this was changed to be more conducive to data protection. Now fingerprints are stored on the card only at the explicit request of the card holder. Card holders should think twice before storing these sensitive data on their identity card; storing fingerprint data yields few recognizable benefits and only a marginal increase in security.

Only government agencies with specially certified devices are able to read the biometric data on the card, for example to conduct police checks of identity.
I am pleased that the electronic biometric data are not being centrally stored except during the production phase, and that no central register for the identity cards is planned. Equally positive is the fact that the government functions are separate from the identity verification functions for e-commerce and e-government.

The electronic identity verification (eID) function is intended to provide greater security and better data protection for Internet users. Using the eID function is voluntary. The eID function is activated in all cards issued to persons over age 16, but it can be deactivated by the issuing authorities free of charge on request and reactivated as needed, for a fee. Card holders should not use their birth date or other insecure series of numbers for their card PIN, which is needed for the eID function. Card holders who wish to use the eID function should make sure that the computer to be used is free of malicious software. This means above all that the computer has a current anti-virus programme and firewall, and that security updates have been carried out regularly.

While I welcome these recommendations, I am critical of the fact that they put most of the burden for the secure use of the eID function on the card holder. Because the

basic card readers do not have their own keyboard, the card PIN must be entered using the computer keyboard. If the computer is infected with spyware, hackers could gain access to the PIN. To avoid this risk, I recommend using the more secure standard or deluxe card readers with the electronic identity card which have their own keyboard and display. Unfortunately, as part of its stimulus package the Federal Government provided subsidies mainly for the more risky basic card readers. One other thing: A deluxe card reader is required to be able to use the qualified electronic signature.

In order to use the eID function, special software, “AusweisApp” must be installed on the computer. The very tight schedule set by the Federal Ministry of the Interior for introducing the electronic identity card may have been one reason why the first version of this software demonstrated security gaps. In particular, there was a possibility that a counterfeit version of AusweisApp could infect users' computers with malware (trojans, viruses). According to the Federal Ministry of the Interior, this problem was solved with the release of a new version of the AusweisApp software.

Companies and public authorities wanting to verify client identity using the eID function must first register with the Federal Office of Administration, which is responsible for checking service providers before issuing them an authorization certificate. The issuing office determines what information on the identity card a service provider needs and what information it will be authorized to read from the card. For users, the authorization certificate reliably identifies service providers. Depending on the purpose of the service offered, the certificate allows different types of access to the card data. For example, in order to verify the age of someone wanting to buy something from a vending machine, fewer data are needed than to conclude a contract for mail-order goods. I welcome this differentiated access based on the principle of necessity as defined in data protection law.

However, I note with some concern the fact that certificates are issued solely on the basis of information and declarations from the service provider. In my view, it would be better if checking the actual data protection standard were required. In addition, consumer protection advocates point out that it is still possible for dubious providers to receive authorization certificates and subsequently cheat consumers, as the Federal Office of Administration is not required to check the business models of service providers.

But in individual cases, card holders may restrict access to their eID data even further than allowed by the authorization certificate. Enabling data subjects to control access to their data is definitely a positive development.

I hope that the issuing authority at the Federal Office of Administration receives the necessary support to ensure appropriate checking. Data protection guidelines for issuing authorization certificates were prepared by a working group whose members included staff from my office, from the Federal Ministry of the Interior, the Federal Office of Administration and the *Land* data protection commissioner.

With the new identity card it is also possible to take advantage of online offerings using an alias: A pseudonym is transmitted instead of the card holder's name. For example, if an online shop uses an online payment service and sells digital goods via downloads, in principle it is possible to buy such products without having to reveal the buyer's name or mailing address.

In addition, a qualified electronic signature function can be optionally activated on the chip, enabling the card holder to sign legally binding documents such as contracts. The card holder must request the qualified electronic signature function from a certification service provider and download it to the chip on the identity card. Downloading and use of the function are subject to a fee.

I will continue to monitor how data protection develops with regard to using the eID function and whether this function and the qualified electronic signature change identity management on the Internet. I will also include in my inspection programme the card readers distributed by the government to read biometric data as soon as larger numbers of these readers are in use.

Because the new identity cards are personalized and issued by local authorities, data protection and IT security for the card largely depend on the organizational and technical conditions at local level. The *Land* data protection commissioners, who are responsible for data protection at this level, found serious shortcomings during the initial phase. I hope that these problems were simply the result of start-up difficulties.

3.3 De-Mail: The secure way to communicate in future?

The De-Mail project introduced reliable, secure and legally binding communication. Although important legal and technical data protection issues were taken into account, some questions remain.

I reported on the De-Mail project (formerly called "citizen portals") in the 22nd Annual Report (no. 6.6). Since then, the Federal Government has adopted a bill governing De-Mail services and amending other legislation (Bundesrat doc. 645/10). At the time of printing, the parliamentary consultations were not yet completed.

The aim of this project is to create an infrastructure for secure and legally binding electronic communications. This infrastructure includes a mailbox and mailing services as well as a secure document safe. Messages are sent via an encrypted channel (see box for no. 3.3 for a diagram). Messages are checked en route for malicious software, and transmission notification is sent, along with delivery confirmation as needed. For proof of delivery, public authorities may request confirmation that the recipient has picked up the message.

During the legislative process, some important improvements were made in terms of data protection: For example, optional end-to-end encryption from the sender to the recipient, in addition to the mandatory transport encryption, was created to protect De-Mails against interception. Clear limits were established for third-party claims to information about the communication and data of De-Mail users.

De-Mail is supposed to be offered only by e-mail providers accredited by the Federal Office for Information Security (BSI). One requirement for accreditation is that e-mail providers have been certified as meeting data protection criteria. The government's draft De-Mail legislation requires the service provider to obtain from a data protection expert an assessment which I will then check. If the assessment meets my approval, I will issue a data protection certificate, which the service provider must present to the BSI as the authority responsible for accreditation.

The data protection examination is based on a catalogue of criteria for which I am responsible. I published a preliminary version of the catalogue of criteria on 19 January 2011; it is available on my website, www.datenschutz.bund.de. The final and binding version will be published in the electronic Federal Gazette when the De-Mail legislation enters into force.

Some data protection considerations have not been taken into account at least so far. Further improvement is needed with regard to the following:

- In future, De-Mail users should be able to save their correspondence with public authorities in encrypted form on the servers of their De-Mail service provider. To

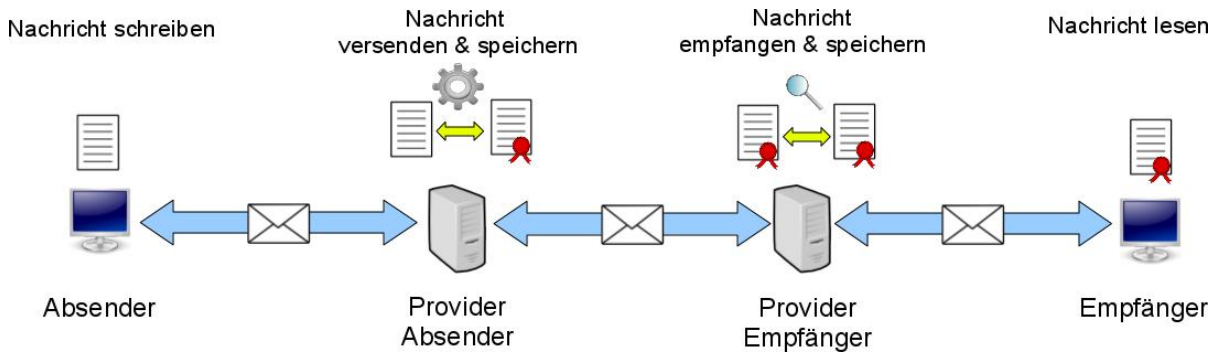
support the secure storage of sensitive documents, De-Mail providers must offer a document safe (“De-Safe”). Users can store documents in the safe, where they are secure from manipulation and loss. To ensure the confidentiality and integrity of this storage, only the user should be able to control the encryption process.

- My demand that the planned retention period of 30 years for logging the opening of the account, every change of data and blocking or closing a De-Mail account was only partly met. Retention periods should comply with the principle of data economy and should be significantly shorter. Another option would be different retention periods for different types of data.

The question remains whether De-Mail or similar services such as the E-Postbrief (see no. 6.8) are appropriate for sending data in need of special protection. In my view, additional protection, such as end-to-end encryption, is needed on top of existing security measures for sensitive data, such as health information.

I definitely approve of the aim of more secure and reliable electronic communication. In this age of electronic mailing of invoices, account statements and access data for websites, it is urgently necessary to provide additional security measures for electronic communications. De-Mail’s acceptance among the public will be the deciding factor. And its acceptance depends on the security, data protection and transparency of the process.

Box for no. 3.3



3.5 Biometrics for border checks

For background checks and border inspections, biometric procedures are to be used to verify identity on the basis of the identity documents presented.

Biometric features have been used in border checks at Frankfurt Airport since 2004. I have repeatedly reported on these biometric checks (see 20th Annual Report, no. 5.3.5; 21st Annual Report, no. 4.5.2). In the absence of electronic travel documents, the Automated and Biometrics-Supported Border Controls (ABG) programme relied on voluntary submission of biometric data, which were stored locally by the Federal Police.

With the introduction of the new electronic passport, it is now possible to use this document to verify identity without prior registration and without having to store the data externally. In 2009, the first tests of automated border checks using facial recognition were conducted at Frankfurt Airport as part of the EasyPASS programme (see 22nd Annual Report, no. 6.4). In terms of technical and organizational framework conditions, a control lane with good lighting for facial recognition was set up. Experience gained from earlier federal biometrics projects was applied to maintain a high level of efficiency in the recognition process. The programme is expected to provide highly accurate recognition and faster identity verification using the data on the passport or new identity card (see no. 3.2) presented, with the aim of reducing the burden on staff and speeding up passenger flows. The inspection process is also intended to create framework conditions in compliance with data protection.

Participation in EasyPASS is currently voluntary, and no prior registration is needed. Every citizen of the EU, the European Economic Area and Switzerland over age 18 and in possession of an electronic passport can take advantage of the EasyPASS programme.

The traveller first lays her passport on a document reader, which reads the data and checks whether the traveller is eligible to participate in the automated check. In my view, it is problematic that in this way every traveller is checked against the national or Schengen database of wanted and missing persons. This is not the intention of the Convention Implementing the Schengen Agreement or the Schengen Borders Code, which state that persons entitled to free movement are not to be systematically checked against national and European databases. I have asked the Federal Ministry of the Interior to evaluate this procedure.
In the control lane, the traveller’s face is photographed. Using facial recognition software, this digital photograph is compared with the facial image stored on the passport chip. At the same time, the authenticity of the passport is checked. If the system finds that the images match and the passport is authentic, the barrier opens and the traveller may cross the border. Federal Police officers monitor the automated

process and may intervene as needed. They also decide whether additional inspection measures are necessary.

The procedure is intended to assist border control personnel in checking travellers, to speed up the inspection process and avoid lengthy waits for travellers.

I welcome the fact that EasyPASS – in contrast to ABG – does not require prior registration by travellers. Nor does it require that travellers' personal data be stored in a database for an unlimited length of time in order to participate. As a result, authorities are not tempted to use these biometric data for other purposes.

It remains to be seen whether the ABG programme will be discontinued if EasyPASS is successful. The ABG framework conditions for frequent travellers (e.g. registration) can also be applied to EasyPASS.

I have monitored the EasyPASS project and the necessary tests and will continue to do so (see no. 7.3.2).

The test phase was completed in 2010 and the procedure approved for routine use. There are plans to introduce the procedure at other airports as well.

4 The Internet

4.1 Locating the individual: Geodata and privacy rights

As expected (see 22nd Annual Report, no. 7.1), the significance of geoinformation has grown enormously – with major consequences for privacy. The combination of geodata and Internet services is especially problematic.

From data subjects' point of view, the huge popularity of smartphones has resulted in countless services ("apps") being offered which use or process location data. The constant combination of one's location with other information has created a new dimension in profiling (see no. 6.2).

When it was introduced in Germany, Google's Street View service was the subject of much discussion. Apart from responding to an extraordinarily large number of comments and questions about this topic, I focused in particular on discussing with policy-makers and the business sectors concerned whether and to what extent the

relationship between processing geoinformation and preserving individual privacy needed to be readjusted (see no. 4.1.1).

The debate only grew when it was revealed that Google had not only taken pictures but had also collected data from WLAN networks in gathering information for Street View (see no. 4.1.2).

The public debate over Google's Street View ultimately led lawmakers to consider whether new legislation was needed on handling personal geoinformation. The Internet industry has presented a geodata code of conduct, while the Federal Ministry of the Interior plans to introduce some fundamental regulations (see no. 4.1.3).

Personal geodata are increasingly collected, processed and used not only by private companies; government has long been interested in geoinformation to help it carry out its tasks. In this area too, the possibilities offered by information technology have a growing relevance for privacy rights.

4.1.1 My home on the Internet: Google's Street View and other services

It is no longer possible to entirely evade the Internet, as many renters and homeowners have found out.

In my last Annual Report (22nd Annual Report, no. 7.2), I described Google's planned Street View service in detail along with its impact on privacy, and called for data protection measures in response. Street View displays digital photos of building facades and property on the Internet, enabling virtual tours. In terms of data protection law, the service is problematic because Google and any other Internet user can combine this information with additional information about residents and owners of the property thus displayed. Street View and similar services thus serve as further sources for increasingly extensive and detailed personality profiles (see nos. 1, 4.1.3, 6.2).

In the meantime, Google has amassed significant amounts of photographic material and has launched its service for Germany; other companies are offering similar services. However, many property owners and residents are concerned about the photographic reproduction of entire streets. Google's announcement that it was launching the service led to intense public debate. Even though my office is not responsible for supervising this activity, I received a relatively large number of complaints, indicating the level of public concern.

The Hamburg commissioner for data protection and freedom of information, who is responsible for this area, and representatives of other supervisory authorities met with Google; after intensive discussions, they were able to get Google to agree to most of the conditions described in my 22nd Annual Report (box for no. 7.2). In talks with the Hamburg commissioner, the company agreed to comply with 13 points (see box for no. 4.1.1). The most important points are automatically blurring images of faces and car number plates before publishing them and allowing data subjects to oppose the dissemination of their personal data both before and after images are made public. These points are required by the Federal Data Protection Act.

Unfortunately, despite intensive coordination with the data protection authorities in other European countries, it has not yet been possible to achieve a comparable level of privacy protection in most of the European countries concerned. This underscores the need to ensure that, as part of its fundamental overhaul, European data protection law also applies to services offered by non-European providers on the European market which have an impact on the data of European residents.

Whereas technical options already existed for individuals to object to the publication of their personal data after the fact, Google had to develop a new technical solution to process requests to opt out of the service prior to publication. This solution had to be able to process these requests quickly and to reliably match them to the photos taken. It also had to be able to prevent fraudulent requests as far as possible.

The solution that was ultimately found had largely positive results for Street View, although it did create some fundamental problems. To opt out of Street View before data were published, data subjects could use an online tool already integrated in Google's map service to mark the relevant point. If specific photographs of this point were found, the data subject was sent a verification code in the mail with which to conclude the opt-out process. By the end of 2010, Google had gone live with its Street View service for Germany’s 20 largest cities.

The problem with the opt-out process is that it provides Google with additional personal data, and supervisory authorities have a difficult time monitoring how Google uses these data: names, addresses and detailed descriptions of homes and property. Numerous comments sent to the data protection commissioners indicated that this kept many persons from participating in the opt-out process; obviously, few people trust Google to handle these data with the proper care.

For this reason, I called for establishing a central opt-out register based at a trustworthy agency (compare no. 4.2) in order to ensure that the opt-out process is as conducive to data protection as possible.

Box for no 4.1.1

13 concessions by Google regarding Street View

The following points are compiled from the measures already included in the service and concessions made to the Düsseldorf Group in April 2009 and to Hamburg's commissioner for data protection and freedom of information in June 2009:

1. Google agreed to use technology to render faces unrecognizable before publishing facial images.
2. Google agreed to use technology to render car number plates unrecognizable before publishing their images.
3. Google agreed to provide a mechanism for residents and property owners to request that a building be removed or rendered unrecognizable, and to process such requests.
4. Google agreed that requests concerning persons, number plates, buildings and property would be taken into account in a simplified form with the result that the corresponding images would be rendered unrecognizable before being made public, on the condition that the property, person or vehicle is identified.
5. Google agreed to publicize in advance on the Internet when and where its vehicles were scheduled to gather photographic data along with a reference to the possibility to opt out. Existing schedules will be published up to two months in advance and constantly updated. Google agreed to specify the list more precisely and to include districts and towns not belonging to a county. The latter have already been added, while districts are to be included by about mid-July 2009.
6. Google agreed that it would still be possible to opt out after images were published.
7. According to Google, the raw data are needed to upgrade and improve Google technology to render faces, vehicle number plates and building facades unrecognizable. Google agreed to erase raw data or render them unrecognizable by substituting the results of the rendering process for the raw data as soon as the raw data no longer need to be stored or processed for the purposes mentioned above.
8. Google agreed to erase or render unrecognizable the raw data of persons, vehicles and building facades which are subject to opt-out requests. These data

will be erased or rendered unrecognizable in the raw data before being made public if Google receives the opt-out request at least one month before the images are made public. In the case of opt-out requests received later or after the images have been made public, the raw data will be erased within two months.

9. Google agreed to draw up a list of data processing operations.
10. If other service providers link to the Street View service, Google reserves the right to terminate such links if applicable law is violated.
11. Google agreed to provide a description of the data processing operations as well as technical and organizational measures for Street View, including in particular a detailed description of how it manages the data of those opting out, from the time an opt-out request is received until the data are finally erased or rendered unrecognizable.
12. Opt-out requests can be submitted via the Internet to www.google.de/streetview or by mail to Google Germany GmbH, Street View, ABC-Strasse 19, 20354 Hamburg. A link to FAQs for Street View and the possibility to opt out is now on the first of the Google Maps Germany help pages. Users can find these pages by clicking on “Help” in the upper right-hand corner of the Google Maps homepage.
13. Google will confirm receipt of opt-out requests without delay. E-mail requests are already being confirmed; letters are being confirmed on an ongoing basis.

4.1.2 Gathering WLAN data

Google’s vehicle-mounted cameras were not only taking digital pictures of buildings; they also gathered data from private wireless networks. Neither the responsible data protection authorities, the data subjects nor the public were informed of this.

During the discussions of Google’s Street View (see above, no. 4.1.1), it was revealed that the company’s image-gathering vehicles were also collecting and storing information from public and private wireless local area networks (WLANs) and transmitting it to the U.S. for further processing. Interestingly, Google collected the WLAN data without informing the responsible data protection authorities, the data subjects or the public. This was confirmed by Google only after a foreign data protection authority found that this was the case after examining one of Google’s camera vehicles and this information became public.

The company argued that it had compiled the locations of wireless networks in order to use this geoinformation later in location-based services (see no. 6.2).

The lawfulness of this WLAN scanning is in dispute, as some of the data compiled constitute personal information: the unique identifier of the WLAN router, or MAC address; the network name chosen by its owner (Service Set Identifier, or SSID); the field strength of the signal; and whether the network is encrypted or not. The SSID in particular may include the network owner's name or even address and thus may clearly identify an individual. But even the MAC address combined with the geocoordinates of the location and signal strength suffices to identify the WLAN's specific address. Especially in less densely populated areas, a wireless network may be tracked to a specific individual. For this reason, my European colleagues and I believe that WLAN scanning requires the consent of the wireless network operators.

And under no circumstances may payload data, that is, the content sent and received via the WLAN, be gathered. Such data can be gathered by WLAN scanners if the network is not encrypted; these data are covered by telecommunications privacy and are protected under the Basic Law. Secretly gathering such information is therefore a criminal offence.

Google initially denied gathering such information from wireless networks, but data protection authorities found that such data had indeed been gathered on a large scale and stored. The data stored included user names, passwords and other sensitive information. Once again, the company confirmed that this was the case only after the fact and publicly apologized for secretly collecting the data.

The Hamburg public prosecutor's office has launched an investigation into this matter.

I find this behaviour by the global leader in the Internet industry scandalous. Google apparently felt that the openness and data transparency it otherwise preaches did not apply to its own practices.

4.1.3 Self-regulation or legislation? A new regulatory framework for geodata services

When it comes to data protection for Internet services, the Federal Minister of the Interior counts on industry self-regulation; lawmakers should limit themselves to defining "red lines". It is doubtful whether the requirements of data protection can be satisfied in this way.

The Federal Government responded with political activity to the ongoing public discussion of Google's Street View (see no. 4.1.1). At a high-level meeting with representatives from industry, politics, data protection authorities and public administration on 20 September 2010 (see also no. 1), the Federal Minister of the Interior recommended that the Internet industry should regulate itself by drafting a data protection code of conduct for dealing with personal geoinformation and coordinating it with the data protection authorities. In the view of the Federal Ministry of the Interior, if this code fulfilled certain conditions, lawmakers would only need to define a "red line" of minimum standards for handling such data in order to prohibit serious infringements of privacy rights. The minister stated that a general right not to have one's personal data published on the Internet was not necessary.

Like my counterparts at *Land* level, I view this approach with scepticism. I see lawmakers as being responsible for ensuring appropriate privacy protection on the Internet, including the handling of personal geodata. This includes introducing a general right to object to having one's personal data published on the Internet.

If this self-regulatory model is to be pursued, a data protection code of conduct must include some minimum requirements such as the general right to object. Above all, such a code must be binding for all companies and enforced by the supervisory authorities (see box to no. 4.1.3).

The industry association BITKOM presented a draft geodata code of conduct on 1 December 2010, the same day the Federal Minister of the Interior made public his ideas concerning a law on minimum standards ("red line"). The BITKOM draft is limited to the publication of panoramas and does not apply to the overall publishing of personal data on the Internet. It provides for a general right to object after images have been published and for establishing a central website where such objections can be submitted. It does not provide for a way to opt out before data are published. The draft provides for sanctions if the code is violated but is binding only for signatories.

Unlike the BITKOM draft, the Federal Ministry of the Interior proposals also target other Internet services, although they are limited to serious infringements of privacy rights. According to these proposals, only the publication of those data should be prohibited that would constitute a serious infringement of privacy, such as data which could be used to create detailed personality or movement profiles, defamatory information or especially sensitive data; the proposals would however uphold freedom of the press.

The federal and state data protection officers have so far had no part in drafting these proposals. BITKOM initiated a process of coordinating with the supervisory authorities in early 2011. Together with my counterparts at state level, I will examine these proposals thoroughly and assist with the process.

No matter how the discussions progress, it can be said that the draft geodata code in particular contains some positive approaches but overall does not satisfy the demands of the federal and state data protection commissioners:

For example, although the code provides for a general right to object to publication, this right can only be exercised after the fact. Effective enforcement of privacy rights, however, would require opting out prior to publication: Once data are out on the Internet, it is very difficult to call them back. In the same way, simply creating a website to coordinate the objection procedures of individual service providers is insufficient and only partly fulfils the call for a central opt-out register. And the binding nature of the data protection code must be significantly improved. Section 38a of the Federal Data Protection Act provides for implementing a binding code of conduct; this procedure should be used. Finally, the proposals so far have entirely overlooked the international dimension of this issue. Service providers active in European markets which process personal data of European residents must also be made to comply with the rules of European data protection, if necessary by revising the European legal framework (see no. 13.2). Making rules conditional on having a subsidiary in Europe or on using data processing means located in Europe is insufficient, as it would not apply to many major Internet companies.
The amendments to the Federal Data Protection Act announced by the Federal Ministry of the Interior are completely inadequate, at least with regard to the creation of personality profiles. It is already unlawful to publish detailed, systematic personality profiles without a legal basis and without the data subject's consent, as such publication would harm overriding interests of the data subject, thereby violating Section 28 of the Federal Data Protection Act. A provision to this effect which was limited to the publication of personality profiles would not improve data protection on the Internet. Instead, what is needed is a ban on creating personality profiles. However, the Federal Ministry of the Interior has so far resisted such a ban.

It remains to be seen whether the Federal Government will introduce the draft legislation announced and how it will be regarded by the Bundestag and Bundesrat.

Box for no 4.1.3

Modern data protection on the Internet: A first step

Joint statement by the Federal Commissioner for Data Protection and Freedom of Information and the North Rhine-Westphalia and Hamburg *Land* Commissioners for Data Protection and Freedom of Information dated 22 September 2010

Participants in the high-level meeting on urban and rural digitization called by Federal Minister of the Interior Thomas de Maizière on 20 September 2010 included the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information, Ulrich Lepper, chair of the Düsseldorf Group of data protection supervisory authorities for the private sector; the Hamburg Commissioner for Data Protection and Freedom of Information, Prof. Johannes Caspar, head of the supervisory authority responsible for several major Internet companies; and the Federal Commissioner for Data Protection and Freedom of Information, Peter Schaar, who together provide the following joint statement:

1. The high-level meeting impressively underscored the significance of data protection in handling geoinformation and for Internet services in general. The enormous diversity of offerings is in sharp contract to the vague and inadequate legal framework for protecting privacy rights. We therefore believe that regulation in the form of clear and binding requirements for protecting privacy is urgently needed.
2. Rules for handling geoinformation can only be a first step towards modernizing data protection on the Internet.
3. Government is obligated to ensure appropriate protection, also in the private sector, of the basic right to determine the use of one's own information. The necessary measures should be covered by legislation without delay. This includes a general right to object to having one's personal data published on the Internet.
4. We view positively the fact that the Federal Minister of the Interior seeks legislation defining the essential minimum requirements for processing personal geoinformation ("red line"). But these requirements must ensure appropriate protection of the right to determine the use of one's data. Voluntary regulation by the Internet industry (data protection code of conduct for geo services) cannot take the place of government regulation. If the Federal Government nonetheless chooses voluntary regulation, this must fulfil at least the following requirements:
   a. A general right to object to having one's personal location data published on the Internet must be created.

b. In order to enable individuals to exercise this right with as little bureaucracy as possible while providing optimal protection for their data, a central opt-out register should be established at an independent and trustworthy agency.
c. Voluntary obligation must be binding for the entire Internet industry.
d. Effective sanctions must be available in case this voluntary obligation is violated.
e. The data protection code of conduct must meet the standard of the results achieved in negotiations between the responsible supervisory authorities and the providers of relevant services (in particular Google's Street View).

5. If the Internet industry is unable to present a voluntary code of conduct which satisfies these requirements in time for the 5th IT Summit on 7 December 2010, legislators must then create the necessary regulations.

4.1.4 Geodata in the public sector

Geodata gathered by government agencies can also infringe on privacy rights.

Government also depends to a large extent on processing geoinformation, for example to provide vital services or for planning or statistical purposes. Further, a number of agencies have the task of gathering geoinformation and making it available for other agencies or the private sector to use. This refers primarily to what are known as basic geodata (see box for no. 4.1.4), but also to detailed and specialized geodata.

In implementing the INSPIRE Directive, the federal and most state governments have passed laws on access to geodata which provide for establishing a national, Europe-wide geodata infrastructure and the right of general access to geodata (see 22nd Annual Report, no. 7.1).

The Federal Government is planning to present draft legislation to govern how federal agencies handle basic geodata. The Federal Ministry of the Interior draft is currently being submitted to the other ministries for their approval; I will also be involved in this process.

In terms of data protection law, the discussion centres on the extent to which geodata are personal data. Data protection law applies only to personal data, to protect individuals. There is no question that basic geodata can be used in a variety of ways which have little impact on privacy. Some have suggested that, if there is no intent to link such information to specific individuals, it is safe to assume that such data are

not personal. In my view, however, orientation on the intended use is risky and the wrong approach in legal terms. According to the Federal Constitutional Court decision on the census, there are no innocuous data. All that matters is whether the data are or can be linked to an individual without unreasonable effort. Excepting supposedly non-sensitive data from the scope of data protection law would have serious consequences: Firstly, if used in a different context these data could very well have an impact on privacy. Secondly, there is a danger that not only official geodata, but all kinds of other data which in certain constellations have only an indirect link to individuals (IP addresses, telephone numbers, car number plates) would no longer be protected.

Given the reduced likelihood and intensity of possible privacy infringement, I believe it is better to facilitate the use of data in certain applications, as in the federal Act on Access to Geodata (which provides for very extensive facilitation). Due to the unresolved question of the relevance of basic geodata for privacy rights, the draft federal Act on Basic Geodata has so far not addressed these issues but leaves general data protection law to solve the problems of data protection.

Box for no. 4.1.4

Geodata keywords:

Basic geodata are those geodata which describe geotopography in a single geodetic reference system in an application neutral way. They provide the basis for specialized spatial applications. Basic geodata include landscape and properties linked with a uniform system of coordinates.

Specialized geodata are those from a certain field of expertise; their spatial reference arises either directly from coordinates or indirectly from reference to basic geodata. They include spatial data relating to climate, population, traffic, the environment, etc.

Geodata are **personal data** when they are specific, i.e. information related to a specific property, which express particular information (e.g. the type and extent of structural use, flooding danger or road access). The prerequisite is that the property owner is a natural person who can be identified without unreasonable effort in terms of time, money or labour.

4.2 The right to object to the publication of personal data on the Internet

Effective data protection requires an attested right to object and an uncomplicated procedure for objecting to the publication of personal data on the Internet.

The photographing of street views and their publication on the Internet by Internet geodata services (see no. 4.1.1) once again demonstrates that existing data protection law does not offer adequate protection against the publication of personal data on the Internet.

Effective data protection requires a binding right to object to the publication of personal data on the Internet. However, any regulations to this effect would have to be formulated in a way that does not infringe the right to freedom of expression guaranteed by Article 5 of the Basic Law. It is lawmakers' responsibility to legislate the key consumer and data protection rights. The data protection code of conduct presented by the Internet industry in December 2010 cannot take the place of a legally attested, actionable right to object, but can have only a supplementary nature.

With regard to the use of geodata on the Internet, as discussed in the case of Google's Street View service, it is clear that rights to object must be flanked by user- and data protection-friendly procedures. So far, data subjects must submit separate objections to each individual geodata service, assuming the service even allows for objections. This requires a significant effort by both data subjects and service providers. Data subjects must repeatedly explain their objection to all services, while revealing additional personal information. And they must constantly be on the alert as to whether a new service intends to publish their data. Service providers must identify data subjects and the relevant properties, which also involves significant effort. Finally, it is even more work for data subjects when the procedures for submitting objections differ from provider to provider.

In the interest of effective and user-friendly data protection, which must equip data subjects with easily exercised and enforced rights, a central opt-out register, for example based at the future data protection foundation Stiftung Datenschutz (see no. 2.5) as a trustworthy agency, could help and ensure that data subjects would have to submit only one objection in order to protect their personal data against publication on the Internet by any service provider. This would also be in the interest of data protection, as providers would not need information identifying the data subject, but only information about the data covered by the objection, in order to comply.

The central information and opt-out agency proposed in the data protection code of conduct presented by the Internet industry in December 2010 (see no. 4.1.3) would not meet these requirements, as data subjects would still have to contact every geodata service provider separately. For this reason, I find it preferable to establish a central opt-out register to object to the systematic publication of identifiable geodata. If experience with such a register proves positive, it could be expanded to further Internet data, for example to opt out of telephone and address registries on the Internet.

4.3 Unnoticed: Web analysis programs in the service of website operators

Providers of telemedia use analysis programs to optimize their website offerings and design. Such programs must meet the data protection requirements given in the Telemedia Act (TMG) and may not be used to track individual user behaviour.

Anyone who offers goods or information on the Internet would like to know how users behave when visiting the website, which pages are accessed most frequently, how users navigate the website and where they exit the website. This is no different in the real world, where marketing psychologists analyse consumer behaviour and both shops and department stores present their wares to appeal to consumers and encourage (or seduce) them into buying.

The digital world on the Internet uses electronic means to perform this task, because users leave digital traces which are easy to analyse. So there are numerous services and programs which website operators can use to record and analyse user behaviour in order to optimize their marketing (on the use of Google Analytics by the statutory health insurance, see no. 4.3.1). These services use different methods: In many cases, the IP address is used to track users' "movement" through a website, or a cookie is set to recognize a returning user. Often, both methods are used – unnoticed by the computer user.

So much for the facts. The Telemedia Act, which applies to Internet offerings, requires two conditions for creating use profiles: They must use aliases, and users must have the possibility to opt out. To clarify: IP addresses constitute personal data, not aliases. And users can exercise their right to opt out only if they are aware of such monitoring, and if an appropriate mechanism is in place to submit an opt-out request. To my knowledge, almost none of the services or programs on offer meets these two conditions.

The Düsseldorf Group of data protection supervisory authorities adopted a resolution summarizing the requirements for web analytics (see box for no. 4.3). Website operators should check to see whether the programs they use fulfil these requirements and if not, they should make changes or use a different product. I have used this resolution as an opportunity to remind the federal authorities once again of what the law requires.

By the way, traffic on my own website is analysed only in anonymous form, as users' IP addresses are abbreviated.

Box for no. 4.3

Resolution of the supreme supervisory authorities for data protection in the private sector
(Düsseldorf Group, 26-27 November 2009)

Data protection-compliant design of web analytics to measure the scope of Internet offerings

Many website operators analyse the traffic on their sites for advertising and marketing research purposes, or to optimize their website design. To create use profiles, they often use software or services provided by third parties free of charge or for a fee.

The supreme supervisory authorities for data protection in the private sector point out that the provisions of the Telemedia Act (TMG) apply to website operators when creating use profiles. According to these provisions, use profiles may be created only with the help of aliases. IP addresses are not aliases as referred to in the Telemedia Act.

In particular, the following rules from the Telemedia Act are to be followed:

- Users must have the possibility to opt out of the creation of use profiles. User opt-out requests must be effectively implemented.
- Depersonalized use data may not be combined with data on persons using an alias. These data must be deleted when no longer needed for analysis or at the user's request.

- In the data protection statement on their website, operators must clearly indicate that they create depersonalized use profiles and that users may opt out of this process.
- Personal data of website users may be gathered and used without consent only where necessary to enable access to telemedia and to calculate charges for such access. Any other use requires the consent of the data subject.
- Because these data may identify specific persons, analysing website usage with the help of complete IP addresses (including geolocation) is permitted only with informed and unambiguous consent. In the absence of such consent, the IP address is to be abbreviated prior to analysis so that is cannot be used to identify a specific person.

If a third party creates depersonalized use profiles, the provisions of the Federal Data Protection Act concerning third-party processing also apply.

4.3.2 Disagreement over IP addresses continues

IP addresses are personal data. Not everyone agrees.

In my supervision of federal agencies, the “old” question whether IP addresses constitute personal data plays a significant role. According to the Federal Ministry of the Interior and the Federal Office for Information Security (BSI), IP addresses do not constitute personal data when accumulated by website operators as usage data. So operators may retain them as long as they like and use them for statistical and data security purposes.

By contrast, I assume that in most cases, IP addresses should be viewed as personal data, because they can be used to identify an individual with the help of additional information. This is also the position of the Article 29 Data Protection Working Party of the European data protection authorities. In its Opinion 4/2007 on the concept of personal data (WP 136, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf), the group finds that IP addresses, whether gathered by access providers or website operators, should be regarded as personal data, as they refer to an identifiable person.

I have already stated that federal agencies are not permitted to retain website users’ IP addresses (see for example 22nd Annual Report, no. 7.9) and called for a change in retention practices. Unfortunately, a significant number of federal agencies refer to

the position of the Federal Ministry of the Interior, which is awaiting the decision in a lawsuit against the Federal Government, represented by the Federal Ministry of the Interior, arguing that the IP addresses of visitors to the websites of federal agencies were unlawfully retained.

In the BSI's opinion, until this lawsuit is resolved, it will also remain unclear in which form usage data may be processed on the basis of the Act to Enhance the Security of Federal Information Systems. The Act does not state whether IP addresses should be regarded as personal data or not. However, one provision covers both eventualities: Protocol data accumulating within the federal communications network must be depersonalized by the BSI prior to processing for purposes of data security only if they contain personal data (see no. 5.2 below).

4.4 A long process comes to an end: The EU telecommunications directives have been adopted

The directives amending directives regulating the telecommunications sector entered into force on 18 December 2009 with their publication in the Official Journal (L 337/11) and must be transposed into national law by 25 May 2011.

The amended directives on a regulatory framework for the telecommunications sector finally entered into force in December 2009. The process of amending the directives, intended to take market developments into account and pay greater attention to consumer interests, had taken more than two years. After tough negotiations on some controversial issues (cf. 22nd Annual Report, no. 7.12), the European Parliament agreed to the reform package.

Some of the changes affect Directive 2002/58/EC on the protection of privacy in the electronic communications sector, known as the e-Privacy Directive. One important addition is the new mandatory notification of personal data breaches: Communications and Internet service providers must inform data subjects if their personal data have been compromised – although only if the breach is likely to adversely affect them. However, the responsible supervisory authority must be notified in every case. This obligation will significantly improve transparency for individual users and will enable them to take appropriate action in case of personal data breaches. This provision introduces for the first time a binding obligation to report violations of data protection. I hope a similar provision will be introduced as part of the amendment of the EU legal framework for data protection in general. General German data protection law has provided for such mandatory notification for

private-sector bodies since the Federal Data Protection Act was amended effective September 2009 (see no. 2.2 above).

Unsolicited e-mails were prohibited already under the old e-Privacy Directive; in an attempt to address growing fraud on the Internet, the new directive expands and specifies the ban on marketing e-mails which violate certain notification requirements (e.g. clearly identifiable, unambiguous and easily accessed conditions for access to a service) with fraudulent intent or which link to such websites. However, I doubt the effectiveness of this provision, as those with fraudulent intent will not abide by it.

During the amendment process, another provision generated discussion: This provision requires the user's informed consent for tracking cookies, which can be used to create use profiles. This would be a major step towards greater transparency and self-determination for users, but service providers and marketing networks regard it as an obstacle to business. At the last minute, and unnoticed by many, wording was added to the relevant recital that consent could also be expressed through the Internet browser setting, if technically possible and effective and if consent could be provided without force, for the specific case and with knowledge of the situation.

Current browsers offer only very general options, however. Further, almost all browsers are preset to accept cookies. Information is almost always lacking. It is obvious that these browsers are so far inadequate to ensure effective informed consent. Even though they would prefer to keep the status quo, website operators and marketers, possibly in cooperation with the makers of Internet browsers, now need to come up with solutions.

The Article 29 Working Party took the same position in its Opinion 2/2010 of 22 June 2010 on online behavioural advertising: It calls for informed consent and sees it as the task of marketing networks to create opt-in mechanisms.

In Germany, the discussion of the "cookie" provisions continues as the directive is being implemented, because the amended directive means that the Telemedia Act (TMG) also needs to be revised. But the responsible Federal Ministry of Economics refuses to do so. The ministry believes that current law already requires consent to set cookies, but neither the wording nor the grounds for the Act back up this position. It also contradicts many years of practice by the supervisory authorities and the general understanding.

In its resolution of 25 November 2010, the Düsseldorf Group of data protection supervisory authorities called for the Telemedia Act to be revised accordingly, thereby lending support to my position (see box for no. 4.4). Perhaps the Federal Ministry of the Interior's legislative initiative concerning data protection on the Internet, the "red line" (see no. 4.1.3 above) will be modified during the legislative process to create clear rules on consent for cookies. Cookies are almost always stored on users' computers to create – often without their knowledge – a profile of their preferences and interests. In my view, this practice oversteps the bounds of what is acceptable and should be prohibited by a "red line".

Box for no. 4.4

Resolution of the supreme supervisory authorities for data protection in the private sector
(Düsseldorf Group, 24-25 November 2010)

Implementing the revised Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

The implementation of the revised Directive 2002/58/EC (e-Privacy Directive) in national law, which must be completed by 24 May 2011, is currently being discussed. The revised directive's Article 5 (3) contains a provision redefining the conditions for dealing with cookies: The previous opt-out solution is to be replaced by an opt-in solution with prior comprehensive information about the purposes of the processing. This change in the directive now requires an amendment to the Telemedia Act, which currently uses an opt-out solution (Section 15 (3) TMG).

Such an amendment has met with significant resistance from the responsible ministry, which regards the general principles defined in Section 12 (1) and (2) of the Telemedia Act as having resolved the consent issue. If one agreed with this interpretation, the current provision would have to be interpreted and applied in a new and stricter way, which would be difficult to explain and likely impossible to enforce.

For their monitoring and supervision in the telemedia field, the data protection supervisory authorities view Section 15 (3) of the Act as key for the use of cookies in this context. According to this provision, use profiles are permitted only under an alias and if the data subject does not object. Use profiles are typically created with the help

of cookies; the unambiguous identification number stored in the cookie (cookie ID) is thus regarded as an alias. This interpretation has proved useful in practice and is generally accepted.

The implementation of the e-Privacy Directive therefore requires a legislative amendment of the Telemedia Act.

4.5 In good hands? In the clutches of social networks

More and more people belong to social networks. So it is increasingly important for them to manage their data carefully. But network operators too must protect the data and privacy of their users.

You don't have to be part of the Internet Generation to belong to a social network, and more and more people are joining, out of curiosity or the desire to know what's going on, or because friends, family or acquaintances have already joined.

During the reporting period, social networks have frequently been in the news, in most cases not in a positive sense. They regularly anger members and scare off potential members with constantly new ideas which do not respect the private sphere.

For example, various social networks changed their terms of use and data protection provisions and set a deadline for members to provide consent, after which they would be dropped. And e-mail addresses uploaded from members' address books were used to find other members with the same contacts, often non-members. In this way, the social networks caught even those persons who did not want to take part. The network operator and third parties used profile data for marketing purposes – without asking, since the data were already there. Most recently, the "like" function on a major American network caused an uproar: Using this little button, which can be found on many web pages, the operator also collects information about what members do and "like" outside the network. And members can see what their "friends" like – a simple marketing strategy.

Given the careless way network operators treat personal data, national and international data protection authorities were forced to respond. Following the Düsseldorf Group and the International Working Group on Data Protection in Telecommunications, the Article 29 Working Group published its comprehensive Opinion 5/2009 on online social networking, which is also available on the Internet

(WP 163, http://ec.europa.eu). The opinion is primarily directed at network operators but also has some helpful information for users.

In the meantime, some improvements have been made: Data protection statements have been revised and structured more clearly, and possibilities to opt out have been added. Once again, I call on Internet users to be careful with their data.

4.6 And now: What has happened to the Act to Impede Access to Child Pornography in Communication Networks?

The Act to Impede Access to Child Pornography in Communication Networks (Federal Gazette I, p. 78) entered into force on 23 February 2010. But the access blocking provided by the law is not being carried out. There are increasing calls to repeal the law.

As soon as the initiative to fight child pornography, launched by the president of the Federal Criminal Police (BKA) and the Federal Minister for Families, became public in early 2009, the plan to block access to the Internet polarized the public, child advocates, victims, legal experts and civil rights advocates. Under the original plan, based on an agreement with the BKA Internet service providers were to filter all Internet traffic and block websites with child pornographic content, showing a stop sign instead of the requested page. The BKA was to update its list of websites with child pornographic content daily and send it to the ISPs via a secure channel.

The subsequent legislative process was very brief and accompanied by sometimes loud and emotional debate. There was and is no question that child pornography must be opposed. But the debate focused on whether blocking access is even effective, as it is easy to get around with a little effort and the necessary expertise. And providers and users of child pornography constantly use normal Internet technology, such as fast flux (see box for no. 4.6), to hide their electronic tracks. This would at least leave in doubt the BKA's daily update of the list. It was also feared that creating the necessary technical infrastructure would open the door to government censorship of other "undesirable" content. And it is obvious that such infrastructure could also be used for commercial purposes.

I found it problematic that checking against the BKA list would require infringement of the privacy of telecommunications without legal authority. The technical implementation of access blocking means expanding the original purpose of DNS lookup (see box for no. 6.4): The traffic data of all Internet users would be subject to

further processing in addition to what was technically necessary. In order to decide whether the stop sign would be displayed instead of the requested web page, every time the page is requested the provider must check whether the page address matches one in the BKA list. However, the discussion did not focus on the proportionality of the measure but on the question of how providers could be reminded of their responsibility. Because a basic right cannot be limited by a simple contractual agreement, legislation was hastily drafted to legalize this limitation.

The law was approved by the Bundestag shortly before the end of the 16th legislative term and was enacted by the Federal President on 17 February 2010 following intensive examination. The Act assigns the Federal Commissioner for Data Protection and Freedom of Information the task of appointing an expert committee within the Commissioner's office to monitor the lawfulness of the entries on the BKA list. I opposed this assignment during the legislative process, because it would interfere with my independence and damage the reputation of my office as an independent data protection monitoring agency. However, this argument failed to influence the majority in the Bundestag.

Then nothing more was heard about access blocking, as in the meantime, the new government had stated in its coalition agreement that it would not enforce the law. Without further ado, the BKA was instructed by decree not to draw up any lists of Internet addresses with child pornographic content, which amounted to non-enforcement. Although I agree with the aim, I question the constitutionality of failing to enforce, by decree, a law passed by the parliament.

Because the BKA did not draw up any lists of websites to block, I saw no further need to appoint an expert committee to monitor such lists.

In response to the petitions of the various parliamentary groups to repeal the Act, a public hearing of the Bundestag Legal Affairs Committee was held in November 2010 in which experts expressed their views on the constitutionality and necessity of a law which requires every Internet access to be checked. It remains to be seen what the parliament ultimately decides.

Box for no. 4.6

Fast Flux

When accessing the website www.bfdi.bund.de, for example, the Domain Name System (DNS) server delivers the IP address 77.87.228.65 to the requesting computer. The DNS is responsible for assigning this IP address to the website, or domain name, www.bfdi.bund.de. The system also allows multiple IP addresses to be assigned to the same domain name. As a result, accessing a domain name returns all the IP addresses assigned to that name. This technique can be used in legitimate networks to distribute burdens.
But botnets, comprised of personal computers infected with malicious software, also use this technique to disguise the location of the servers where the illegal content is actually stored. In this case, one domain name may be assigned hundreds or even thousands of IP addresses of infected PCs which are changed rapidly in these networks. The different IP addresses are provided to the requesting computer according to a certain method – sometimes this one, then that one. In this way, the request is sent first to an infected PC. Because the infected PCs are manipulated to operate as signposts to the server where the illegal content is actually stored, they provide the requesting computer with the correct IP address, where the illegal content is then accessed.

4.7 ACTA: No data retention for possible future use in the private sector

An international requirement for telecommunications service providers to monitor their customers and provider liability for illegal customer behaviour were stopped.

The Anti-Counterfeiting Trade Agreement (ACTA) is an international agreement between the European Union, its member states and other countries, including Australia, Japan, Canada, Mexico, Switzerland and the U.S., intended to increase protection of intellectual property and copyright on the Internet. It is supposed to supplement existing World Trade Organization agreements and set an international standard for protecting and enforcing intellectual property rights. The European Commission represented the EU member states in the negotiations, which lasted over three years and were initially conducted in secret. Only after protests from civil rights advocates did the Commission decide to publish comprehensive documentation on its website in April 2010. After agreement had been reached on almost all the major issues at the closing conference in Tokyo in early October 2010, the final text of the agreement, dated 3 December 2010, was made public.

The consultations focused among other things on requiring telecommunications services providers to monitor users of their services for possible violations of

copyright law, for example. If providers failed to conduct such monitoring as required, they were to be liable for any violations committed by their customers. Because providers would have to store relevant data in order to monitor customer behaviour, from the perspective of data protection law, this would mean storing IP addresses and telecommunications traffic data of non-suspicious persons without specific grounds. Ultimately, however, this provision was left out of the agreement.

I view the overall result of negotiations as a victory for data protection law. ACTA is to be ratified by the individual parties to the agreement in the coming months.

4.8 Identifying IP addresses to fight copyright violations

Internet service providers do not violate data protection law by providing, in response to a court order, the names and addresses of persons assigned a specific IP address at a particular time. This practice by copyright holders nonetheless raises questions.

During the reporting period, a large number of individuals contacted my office after receiving warnings from copyright holders; these individuals complained that their Internet service providers (ISPs) had revealed their names and addresses to the copyright holders without their knowledge.

From the perspective of data protection law, there is nothing wrong with ISPs releasing customer information in response to a court order. Such information may be released only on the basis of a court order under Section 101 (9) of the Copyright Act (UrhG). Without such an order, the ISP may not release this information to private third parties. Based on the complaints concerning this issue, I realized that the public is not aware that, under current law, ISPs are **not** required to inform their customers when they release this information. ISPs are not allowed to keep a record of such releases, so they cannot inform customers upon request.

The release of customer information occurs in two steps: First, the court issues an order not to delete the data. Next, after checking whether the situation meets the conditions given in Section 101 of the Copyright Act, the court issues the order to release the desired information to the party who has requested it. If the data have already been deleted at the time the court issues the first order, then the copyright holder will not receive any information. This may happen, as ISPs are supposed to delete user data immediately after use and are therefore allowed to keep access data for only a short time (no more than seven days) where necessary for billing purposes, to limit technical faults and to investigate abuse.

My office is unable to investigate whether an individual did in fact unlawfully download a copyrighted work from the Internet; in this case, recourse is possible under civil law.

Regardless of this legal situation, however, the question arises as to whether storing and analysing massive numbers of IP addresses gathered from filesharing sites as practised by specialized companies and legal firms violates the principles of data economy and transparency. And the form-letter and often unspecific requests for information leave a bad taste in the mouth.

I am also very critical of calls to use data retained for possible future use on the basis of legal provisions and for the purpose of investigating serious crime (see no. 6.1) also to combat copyright violations. Fortunately, the Federal Constitutional Court has put a stop to such plans.

4.9 The Joint Internet Surveillance Centre of the security authorities

The work of the Joint Internet Surveillance Centre (GIZ) infringes the right of data subjects to determine the use of their own data.

The Joint Internet Surveillance Centre is a forum for cooperation in which the participating agencies (Federal Office for the Protection of the Constitution, Federal Criminal Police Office, Federal Intelligence Service, Military Counterintelligence Service and Federal Public Prosecutor General) pool their subject-specific, linguistic and technical resources to search the Internet for indications of extremist and terrorist activity.

To this end, the participating agencies monitor in particular Islamist websites, relevant newsgroups, forums and chatrooms and analyse what they find. This information is compiled in periodic or special reports (known as a GIZ-LOG) and provided to cooperation partners. In a speech introducing the centre in October 2007, the Federal Minister of the Interior explained that it monitored only the publicly accessible Internet and that its task therefore required no special sovereign authority.

What seems plausible at first glance becomes inconsistent upon closer observation. On an advisory and supervisory visit to the centre in December 2009, I looked into

whether its activities infringed on the rights of data subjects to determine the use of their personal data.

In its judgement of 27 February 2008 on remote searches of computer hard drives (1 BvR 370/07; see also 22nd Annual Report, no. 4.1.1), the Federal Constitutional Court found that the government may take note of publicly accessible information. This also applies to personal information gathered in individual cases, for example by participating in chat and discussion forums using a pseudonym, as long as the government agency does not exploit the legitimate trust of the data subject in the identity and motivation of the person with whom he or she is communicating. That means: As long as a security agency affiliated with the centre is active in chats or forums in which a fictitious name and password can be used to register, the legitimate interest of data subjects is not affected.

However, if security officers supply fictitious detailed personal information, such as a fictitious name, address, telephone number, e-mail address, etc. disguising their affiliation with a security authority when registering to participate in a chat or discussion forum, then legitimate trust is affected. In my view, officers' active participation in chats and forums also exploit the legitimate interests of communication partners. Because some communication platforms require members to submit comments in order to maintain their membership, the agencies in the centre must submit comments in order to retain access. By doing so, for example when answering questions from another member of the forum, they may create the false impression that they actively support the community.
Although it may be difficult in individual cases to determine at what stage Internet surveillance by the authorities exploits the legitimate trust of data subjects in their communication partners, the court's judgement mentioned above assumes that the individual's right to determine the use of his or her own data is infringed whenever the collected data are purposely compiled, stored and analysed using additional data. This is precisely the task and aim of the Joint Internet Surveillance Centre. The participating security agencies therefore need a legal basis for their work (see also no. 7.1.7).

4.11 Improving international cooperation on data protection

In view of the growing global streams of data, closer cooperation among national data protection authorities is assuming increasing importance. Various initiatives in

which I have actively participated have been launched to improve international cooperation.

In April 2010, ten national data protection authorities wrote a **joint open letter asking Google** to do a better job of protecting user privacy in its new Buzz service.[1] With Buzz, Google expanded its existing e-mail service, G-Mail, into a social network. The letter criticized in particular the fact that the new service revealed users' personal data without sufficiently informing them beforehand, so they were not in a position to decide for themselves how their data should be used. Google publicly apologized for the data protection violations which occurred with the introduction of Buzz.

Also in spring 2010, the **Global Privacy Enforcement Network (GPEN)** was founded as an informal association of national data protection authorities. The aim of the network is to improve international cooperation on enforcing data protection law. Planned activities include regular sharing of experience among members and advanced training together with representatives of industry, academia or international organizations. Bilateral support and cooperation measures are also to be agreed on. The network has agreed to hold telephone conferences on a regular basis and to meet on the margins of international conferences, such as the International Conference of Data Protection and Privacy Commissioners. In addition, the GPEN has launched a website with OECD support to assist with the network's activities. The website has both a public and a members-only area (see www.privacyenforcement.net).

Four **case-handling workshops** were held in 2009 and 2010, in which staff from my office took part. These workshops were created by the European Conference of Data Protection Authorities to share experience and insights and in this way to arrive at a consistent approach for dealing with similar issues and citizens' queries. The case-handling workshops differ from other forums for European cooperation in that the target audience is primarily staff from the data protection authorities (case officers) who deal with specific problems and questions. The two most recent workshops were held in Brussels (March 2010) and Manchester (September 2010) on data protection in research and the health-care sector, data protection in modern mobility systems and efficient ways and methods to process cases and complaints. The case-handling workshops are open to staff of data protection authorities in all European countries, not just EU member states.

---

[1] The joint letter was signed by the data protection authorities of Canada, France, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, Germany and the U.K.

5 Technological data protection

Even though data protection has traditionally been understood primarily as a legal matter, the significance of technology for both threats to and protection of privacy continues to grow.

Protecting data through technology: This theme has permeated the annual reports of the federal and *Länder* data protection commissioners for many years. Nonetheless, it is anything but old hat; on the contrary, even IT specialists and users who don't ordinarily pay much attention to data protection seem to have heard that new products, services and business models need protective mechanisms. Anyone who has not yet heeded this lesson should take a closer look at the data protection scandals and spectacular cases of data misuse, especially with regard to the image of the companies concerned and to the potential for harm.

Technological data protection and commercial success – this can even be a win-win constellation, at least when the competitive edge in terms of data protection is used as a marketing tool. This is another reason I have long advocated data protection audits, or certificates of approval for those products, services and companies which guarantee an especially high level of data protection. Certification of technical systems using protection profiles (see for example 22nd Annual Report, no. 8.1) also falls into this category.

Data protection and IT security go hand in hand, at least most of the time, such as when developing new security standards for mobile communications (see no. 5.11). But sometimes conflicts arise, for example when government agencies use the argument of increasing IT security when calling for additional possibilities for surveillance.

Issues of technological data protection come up in every chapter of this report. It is a core element in the modernization of data protection law (see no. 1), is reflected in measures to further develop the framework of data protection law (see nos. 2.3 and 2.4) and has been incorporated into plans for a data protection foundation, the Stiftung Datenschutz (see no. 2.5). Electronic identity (see no. 3) is also an issue of technological data protection, along with the Internet (no. 4). Whether telecommunications and postal services (no. 6) or internal security projects (no. 7), technological issues arise everywhere. There are numerous projects requiring technological data protection expertise even in the areas of internal administration

and legal affairs (no. 8), finances (no. 9), business and transport (no. 10), health and social affairs (no. 11) and protection of employee data (no. 12).

It takes people to provide technological data protection, so I am very pleased that I was able to add IT specialists to my team during the reporting period (see no. 14.4), significantly improving the technical advisory and inspection competence of my office.

It is hardly surprising that the Federal Government also has interministerial projects addressing data protection issues, although the results so far are sometimes less than entirely satisfying.

The fifth national IT summit, an annual meeting of high-ranking representatives from the world of politics, business and research, was held in 2010 in Dresden. Unfortunately, the summit rarely devotes enough attention to data and consumer protection issues. One could have expected more from the 2010 IT summit in particular, The discussions this year focused on the new ICT strategy “Deutschland Digital 2015”, but paid little attention to public interests concerning data and consumer protection. For this reason, the board of the Federation of German Consumer Organizations (vzbv) and I published a five-point catalogue ahead of the IT summit, so that large-scale digital projects could not ignore data and consumer protection concerns (see box a for no. 5).

During the reporting period, the IT Planning Council was created to coordinate IT issues among the federal, state and local governments. The necessary article in the Basic Law, Article 91c, was added in August 2009 (see box b for no. 5). As the adviser to the Council, I supported including a representative of the *Land* commissioner for data protection.

At its meeting on 24 September 2010, the IT Planning Council adopted the National E-Government Strategy. Thanks in part to my involvement in preparing this strategy, data protection and freedom of information were included as one of its six central goals. For example, the strategy states that relevant applications must pursue the goals of data reduction and data economy, and that administrative services should be available to users anonymously or with an alias if possible. The plans to bundle tasks and establish cross-level cooperation between various administrative bodies and authorities can be carried out only with strict adherence to privacy rights and the principle of separation of informational powers.

The National E-Government Strategy also contains the obligation to make appropriate policy and administrative information available to the public, thereby bringing the idea of open government to life. In view of my second area of responsibility, freedom of information, I am especially pleased about this.

Box a for no. 5

Five-point catalogue

1. Strengthening technological data protection
   When new technologies are being developed, data protection must be taken into account early on (privacy by design). Preferences for social networks and Internet browsers should be pre-set to provide a high level of data and consumer protection (privacy by default).

2. Making data collection and processing more transparent
   Information about technologies used to gather and process data must be appropriate to the context, understandable and easy to access. Consent to gather and process data should remain valid only for a limited period of time. Active, informed consent should be required to gather and process data.

3. Improving the legal framework
   Key rights of consumer and data protection should be covered by law. This includes an attested right of data subjects to opt out of having their data published on the Internet and a ban on creating profiles without the data subject's consent.

4. Making voluntary self-regulation more binding
   Voluntary self-regulation, such as the data protection code of conduct recently presented by geodata services (including Google’s Street View), are to be welcomed. However, they must be accompanied by monitoring and sanctions in case of violations. Self-regulation is no substitute for an attested, actionable right to object.

5. Enforcing consumer and data protection internationally
   Even though it takes place locally, Internet surfing is a global affair. Internet services covered by the Safe Harbor Agreement must comply with European and national law and must inform users of this fact. To achieve this, the agreement must be improved and effectively enforced.

Box b for no. 5

Article 91c of the Basic Law

(1) In planning, setting up and operating information technology systems needed to carry out their tasks, the Federation and *Länder* governments may work together.

(2) On the basis of agreements, the Federation and the *Länder* may define standards and security requirements needed for communication between their information technology systems. Agreements on the basis for cooperation under (1) may, for individual tasks depending on their content and scope, require that more specific rules enter into force for the Federation and the *Länder* upon approval of qualified majorities, to be determined in the agreement. They require the approval of the Bundestag and the parliaments of the participating *Länder*; the right to terminate these agreements cannot be ruled out. The agreements shall also govern the responsibility for costs.

(3) In addition, the *Länder* may agree to operate information technology systems jointly and to set up the facilities for that purpose.

(4) The Federation shall create a network to connect the federal and *Länder* information technology networks. A federal law subject to Bundesrat approval shall govern the details of setting up and operating this network.

5.1 Smart metering: The intelligent electricity meter

Ensuring a sustainable energy supply is an important goal which includes efficient and environmentally friendly production and distribution – but not at the price of transparent energy consumers.

Sustainability depends on the widespread use of renewable energy and on greater energy efficiency. Producing energy from renewable sources creates new challenges for energy suppliers and requires intelligent connections between energy production, transport, storage and consumption. Smart grids and the use of new metering and management technology is intended to ensure that the right amount of power is produced just in time and can be delivered without the need for expensive storage. To do so, more usage and management information is necessary than can be provided by conventional, analogue metering and management technology.

A first step towards more efficient energy production and consumption is user rates which create incentives for individuals to manage their energy use and thereby cut consumption. To display actual consumption and time of use, thereby enabling a more effective use of resources, Directive 2006/32/EC requires new "smart" meters to be provided in all EU Member States. As a result, Section 21b (3a) of the Energy Industry Act (EnWG) requires such smart meters to be used in all new construction and major renovations since 1 January 2010, so that consumers can take advantage of economy rates to be offered by 1 January 2011 at the latest.

Many of our activities at home, at work and in our leisure time rely on technology and are reflected, depending on the devices we use, in patterns of energy consumption and time of use. Measuring energy consumed by various devices makes it possible to develop an increasingly precise picture of individual and highly personal activities. Each activity can be recognized distinctly and in real time. Over the course of a day, this yields a record of activities containing key information for a behaviour profile. It is therefore obvious that these new metering and energy conservation technologies must comply with data protection law in order to protect the privacy of energy consumers.

“Privacy by design” is the keyword for such data protection-compliant solutions. It means first of all recognizing and questioning the impact of future information technologies at an early stage. Privacy by design also means acting on this awareness and reducing the risks and threat of misuse not only through legal measures such as bans and penalties, but also by incorporating data protection into the design as early as possible (see also no. 3.1).

For smart metering to comply with data protection law, this means assessing the need for every plan to gather, record and use personal data; depersonalizing data at the lowest step of the system at the earliest possible stage; and ensuring complete transparency and unlimited data autonomy for consumers. Consumers should not be forced to accept a "black box” whose data storage, evaluation, transmission and remote control functions they do not understand. Data subjects must retain control over their consumption data.

The Conference of Data Protection Commissioners of the Federation and the *Länder* found a lack of data protection legislation covering digital metering and management of energy consumption (see box for no. 5.1). Current legislation on the introduction of digital meters does not adequately protect consumers’ privacy. The Conference

therefore calls for legislation covering the collection, processing and use of digitally collected information on energy consumption.

I have asked the parliament and the Federal Ministry of Economics and Technology to support smart metering that complies with data protection law and ensures secure information processing. At my suggestion, that ministry and the Federal Office for Information Security (BSI) have started working on secure protection profiles for the new metering technology. The Energy Industry Act is in the process of being amended; the new version will also contain provisions on smart metering. During the legislative process, I will insist that these provisions satisfy data protection law.

Box for no. 5.1

Resolution of the 80th Conference of Data Protection Commissioners of the Federation and the *Länder* of 3/4 November 2010

Data protection for the digital metering and management of energy consumption

The Energy Industry Act requires that, starting in January 2010, digital meters which measure actual energy use (e.g. electricity and gas) and the actual time of use must be used in homes (smart metering). These are intended to enable consumers to monitor and control their energy consumption better and to help improve energy efficiency.

Digital meters make it possible to measure consumption to the second. This information is personal data which can be used to create detailed usage profiles. Many activities in daily life at home use energy, at least indirectly, so using these resources also reflects daily routines. For this reason, tracking consumption in detail creates enormous potential to track individuals' daily habits. This applies especially when energy consumption of individual devices is measured in addition to overall household consumption. Enhancing digital meters to control household devices creates additional risks.

Tracking energy consumption in detail can result in serious violations of privacy and interfere with the right to determine the use of one's own information and the constitutionally guaranteed inviolability of the home. Additional threats to privacy may result from long-term recording of this information, the possibility to link such usage profiles with other data, and the remote monitoring of data.

Efficient energy supply and use must not have a negative impact on data protection. But current legislation on the introduction of digital meters does not adequately protect consumers' privacy.

The Conference of Data Protection Commissioners of the Federation and the *Länder* therefore calls for legislation covering the collection, processing and use of digitally generated information on energy consumption. This legislation must respect the legitimate interests of data subjects and require that the personal data collected are subject to strict restrictions on use. The legislation must also ensure that the principles of transparency in data processing are upheld and that rights of data subjects are protected.

Ensuring data protection must be incorporated into the planning and design of the infrastructure and technical facilities for measuring energy use. This applies in particular to the principle of data reduction and to data subjects' sovereignty over their own data. For example, detailed data on energy consumption of individual devices must be processed under the exclusive control of data subjects and must not be transmitted to third parties in a way that allows individuals to be identified directly or indirectly. All consumers should be able to take advantage of environmentally friendly and less-expensive energy rates without having to reveal profiles of their personal energy consumption.

State-of-the-art technical and organizational measures are to be taken to ensure that digital meters and smart grids preserve confidentiality, integrity, availability and transparency when processing energy consumption, management and other data. This includes encrypting personal consumption data. Binding standards for technological data protection and IT security should be defined in line with the sensitive nature of the data and the anticipated risk of misuse. An integrated data protection and security management system should also be created for the data processing systems.

5.3 Privacy framework/technical standardization

Many technical processes and products must meet data protection requirements. Standards for these processes and products must therefore also meet these requirements.

The standardization of technical processes has become more important in recent years. The globalization of markets has increased the demand among device manufacturers and service providers for global standards. Many technical standards also have ramifications for data protection, although these are often recognized only after the fact. Together with foreign data protection authorities and *Länder* data protection commissioners, I have therefore decided to become more involved in developing these standards, both international (ISO) and German (DIN) standards.

For example, I am currently assisting with the revision of DIN 32757 on the secure destruction of digital storage media. If personal data are stored on digital media, these media must be securely destroyed to ensure the effective erasure of the personal data. Due to the miniaturization of data storage media and the growing information density (number of bits per surface), DIN 32757 is no longer able to keep up with current technology. As storage media have become less expensive, there is less and less incentive to delete data. I have therefore decided to assist with revising these provisions in the working group on the destruction of digital storage media, part of the information technology and applications standards committee of the German Institute for Standardization (DIN). Since 1995, the DIN 32757 standard has defined terms and set minimum standards for machines and facilities with regard to the destruction of digital storage media in five levels of security. These levels are characterized by particular cutting widths and lengths which are based on the technology on the market at the time.

For example, cutting widths for paper media are based on printers and font sizes current when the standard was created. With the dot matrix printers common at the time, shredding according to security levels S1 through S5 yielded acceptable results for data protection purposes. This is no longer true for today's printers and font sizes. Today's smaller and more readable fonts also reduce the amount of paper needed, and this economic incentive means that these fonts are increasingly used. When it comes to destroying paper, however, this means that the cutting widths specified in the standard no longer satisfy data protection requirements: Sometimes longer sections are still legible on the remaining paper strips.

The same applies to digital storage media. For example, a DVD can store four times more information than a CD. With other storage media as well, miniaturization means that the cutting widths for destruction are no longer adequate. For example, the old DIN 32757 is sufficient for a classic SD memory card, which is 32x24mm, but levels S1 to S2 would not be able to safely destroy a microSD, at 11x15mm, because the cutting width is too large.

These examples show that revision is urgently needed in order to meet data protection requirements when new devices are being developed. Another consideration with regard to destroying storage media that must be taken into account has to do with the question of recycling the destroyed media. In recycling, the following rule applies: the larger the remaining parts, the better they can be recycled. But this rule runs contrary to data protection requirements, because larger parts also contain a greater density of information. Everyone in the working group agrees that the previous five levels of security are no longer sufficient and that at least a sixth level will be needed in the future.

The discussions are ongoing and are scheduled to be completed in spring 2011. I am optimistic that the data protection requirements will be met.

5.4 Collected once, stored forever? Problems with data deletion

Personal data must be deleted when they are no longer needed or when they are stored without authorization. Unfortunately, not all IT systems meet these legal requirements.

SAP software helps manage goods, services, staff and customer data. The federal administration increasingly uses SAP software to automate its business processes. In some installations, it has proved impossible to delete personal data from SAP systems.

According to the Federal Data Protection Act, personal data are to be deleted when they are no longer needed or if their storage is not permitted for other reasons. The Act defines deletion as rendering stored personal data unreadable. This is achieved neither by logically deleting the data, while leaving open the possibility of restoring them, nor by preventing the possibility of searching for them.

On various occasions, I have found that procedures based on SAP R/3 (especially with the HR module for human resources management) fail to meet the requirements of deletion in line with data protection law (see also nos. 5.4.1 and 5.4.2). For this reason, I sought a general overview of the use of SAP systems within my area of responsibility. Using a questionnaire to this effect, I gathered information on the use of SAP systems and the kind of personal data processed using such systems (e.g. customer data, human resources data, data on sickness allowances for civil servants, budget data). I also wanted to know whether a data protection strategy had been developed and whether processing instructions existed.

In examining the questionnaire responses, I found that the federal administration uses SAP products in only a few cases. Where these products are used, however, personal data are affected, often those in need of special protection, such as data from personnel files and human resources data. With regard to deleting personal data, the results were worrying: Many government agencies have so far assumed that the data within the system can be deleted. Not all were aware that SAP software is not always able to delete data. My initiative seems to have caused the agencies concerned to reconsider the matter and examine the existing deletion routine more critically. Based on the sobering results of the questionnaire – data are not always deleted properly according to data protection standards – I contacted SAP directly in order to work with the software manufacturer to find a solution. SAP agreed to provide a module in 2010 for deleting data which might solve the problem. SAP reported that the module was available in the software SAP R/3 4.7 Enterprise, and that the agencies concerned had installed and tested the module. However, the anticipated success failed to materialize. The module delivered by SAP did not delete any data and in some cases caused problems with the database. In this case, the data had to be deleted manually. As a result, I will discuss this problem with SAP at length in spring 2011. If the situation does not change, I will no longer be able to endorse the use of SAP products.

5.6 Cloud computing: Data protection in the cloud?

Cloud computing – the provision of computing capacity over the Internet – raises many data protection issues.

Cloud computing refers to the dynamic provision of resources such as computer capacity, data storage or ready-made program packages over networks, especially the Internet. Cloud computing services claim they save money and offer greater flexibility; but it is unclear how they ensure data protection and data security.

Cloud computing in its purest form, as an open, global model, is difficult to reconcile with current data protection law. If a data controller, a client of cloud services, decides to store personal data on servers around the world, this approach soon reaches its limits. In the extreme, the controller does not even know who is technically processing the data or where. So restrictions on the use of cloud computing are needed.

In most constellations, controllers do not want to delegate responsibility for their data, so according to the European Data Protection Directive and the Federal Data Protection Act, the situation is regarded as a form of third-party data processing. In this case, according to Section 11 of the Act, the responsibility for data protection typically remains with the controller. This means that a series of legal, formal, technical and organizational requirements must be taken into account (see also no. 2.4 on third-party data processing). In cloud computing it is necessary to pay attention to the following:

Processing may be shifted to the cloud only when delegating data processing procedures to private third parties as third-party processing is permitted. It is necessary to abide by restrictions for specific areas, such as social legislation.

Processing in the cloud does not usually remain within Germany's borders. The same standards as in Germany apply to foreign processors only if these processors are based in the EU or in countries of the European Economic Area, or if the data are processed in these countries.

For third parties which process the data outside the EU or the EEA, it is necessary to ensure appropriate data protection in the relevant third countries and possibly gain permission from the data protection authority responsible for the data controller. The same standards as for data transmission to a third country apply to the suitability of these measures.

The requirements specified in Section 11 of the Federal Data Protection Act must be met whether the processor is German or foreign. For example, the written contract must specify the subject and length, scope, type of data and groups of data subjects, the technical and organizational measures, rules for correction and deletion and additional measures under Section 11 (2) of the Act. This means that the controller must know in detail which data are processed where and under what conditions. This is difficult to achieve in cloud computing, where available server capacity is assigned ad hoc.

Before data processing begins and regularly thereafter, the controller must make sure that the processor complies with the technical and organizational measures to ensure data protection, whether through local inspections or certification by an independent, neutral and trustworthy third party. The conditions of the individual computing centres and the local conditions must also be inspected.

The data processor must also ensure effective data protection inspections. Various practical difficulties are likely here as well due to the dispersed approach.

For these reasons, cloud computing is currently permitted and practical only under restrictive conditions.

One solution would be a provision on joint data processing of several data controllers. The concept of accountability might be helpful in this regard. Accountability means that if more than one body is involved in data processing, legal provisions should make the responsibility for the lawfulness of data processing depend on the actual possibilities for exerting influence and the interests of the data subjects. In its outline on modernizing data protection law, the Conference of Data Protection Commissioners of the Federation and the *Länder* has already presented initial recommendations (see no. 1).

Responsibilities must be distributed in a way that does justice to different interests; in the case of cloud computing, this means those of the processor(s) as well. Every body which in fact can determine means and purposes of data processing should be responsible to that degree for the lawfulness of the data processing.

Services should be performed in the cloud only when certain legal, technical and organizational conditions are met (see box for no. 5.6). Personal data may be processed in the cloud only when they are effectively protected against misuse. The principle of privacy by design should also be followed here, in order to implement effective data protection at an early stage, i.e. when cloud services are created. In addition, a high level of transparency must be assured when using cloud services. Overall, I still see many unresolved legal and technical questions in relation to cloud computing.

Box for no. 5.6

A set of guidelines for **using cloud computing**, "BSI minimum standards for providers of cloud computing services", is currently undergoing the public approval process. This document (version 0.96 of 27 September 2010) lists basic requirements, requirements for a high level of confidentiality and of availability on the basis of basic IT protection when using cloud computing. Among other things, it considers the provider's security management, security architecture, ID and rights management, transparency, organizational requirements, possibility for user monitoring and data protection/compliance. These guidelines are intended to enable

providers of cloud services to deal with an issue as complex as the use of cloud computing from the perspective of IT security.

5.8 Electronic engine control units: Cars as computers on wheels

Electronic engine control units in cars are intended to improve vehicle safety and assist with maintenance. At the same time, however, there is a growing risk that this trend could result in the "transparent driver".

From humble beginnings about thirty years ago, cars are now equipped with increasingly complex and powerful electronic aids and data recorders. Most car owners and drivers know very little, if anything, about them or how they work. Some of the data generated, such as those related to technical engine management, have little to do with identifiable individuals. However, when further, behaviour-related information is recorded, the threshold of being able to identify specific persons is quickly reached. This applies for example to the frequency distribution of readings on speed, (lateral) acceleration, vehicle position, braking and the resulting deceleration rate.

Ordinary cars today have between 40 and 60 engine control units (ECU) connected to an engine management system. The recorded data can be retrieved by car repair shops and manufacturers from a central port. Data used for car maintenance provide information on the driver's acceleration, speed and braking behaviour, resulting in a detailed vehicle-use profile and possibly also driver profile. If these are combined with online data, such as geolocation via GPS, the "transparent driver" becomes increasingly likely.

Repair shops are permitted to use these data for repair and maintenance work at the car owner's request, if the car owner is also the driver and has access to understandable information about the data recorded in the ECUs before requesting the repair/maintenance work, either from the owner's manual, sales contract or repair/service contract. The same applies to the collection, processing and use of vehicle data from the data recorder which only the manufacturer is able to access.

General remarks such as the following do not constitute "understandable information" as referred to above: "Your car records data on its operation, problems and user settings. These data are stored in the vehicle and can be retrieved using appropriate

devices, particularly when servicing the vehicle. The data are used to assist with service and repairs or to optimize and enhance vehicle functions."

The Düsseldorf Group has addressed the data protection problems associated with electronic engine control units and has established a working group, to which I belong. This working group first analysed the collection, processing and use of vehicle data in light of their ability to identify specific persons. This analysis is intended to improve information for data subjects provided in owner's manuals, sales contracts and repair/service contracts. The necessary work was still in progress at the time this report went to press.

5.9 RFID PIA at European level

In order to analyse data protection risks and impacts associated with the use of radio frequency identification (RFID), a strategy for privacy impact assessment (PIA) was developed at European level. In future, industry, trade and businesses using RFID are to produce PIA reports and submit them to the national supervisory authorities for examination before beginning RFID operations.

RFID is taking over the world while largely escaping the public's notice. RFID chips are now integrated in clothing made by well-known manufacturers, in customer loyalty cards and in Germany's new identity card. The RFID Information Forum recommends that products containing RFID chips should be marked with a logo chosen in a contest (see box a for no. 5.9). All passports containing RFID chips in accordance with the ICAO standard are marked with a logo (see box b for no. 5.9). I reported at length on the RFID issue in my latest annual reports (see most recently 22nd Annual Report, no. 6.7).

The European Commission's strategy calls for developing guidelines for technology impact assessment for RFID systems (RFID PIA). Developing an RFID PIA is based on the recommendation of the European Commission dated 12 May 2009, 2009/387/EC (L 122, p. 47), which states that several principles should be followed when using RFID.

These include:

- special marking of goods containing RFID tags;
- using the same logo Europe-wide to indicate the use of RFID;
- general information on the use of RFID;

- automatic deactivation of RFID tags at the point of sale.

In line with the opt-in principle, RFID tags should be allowed to continue transmitting after the item has been paid for only at the customer's explicit request. RFID reading and writing devices and communication processes should be clearly apparent to customers. There should be comprehensive information about which personal data are processed for what purposes.

Before going into operation, RFID systems should be subject to impact assessments to determine whether they comply with data protection requirements. And a report should be submitted to the national data protection authorities at least six weeks before the systems are to go into operation. This (non-binding) recommendation, based on an online consultation in 2006, is intended to create the same starting conditions for RFID manufacturers and users throughout Europe.

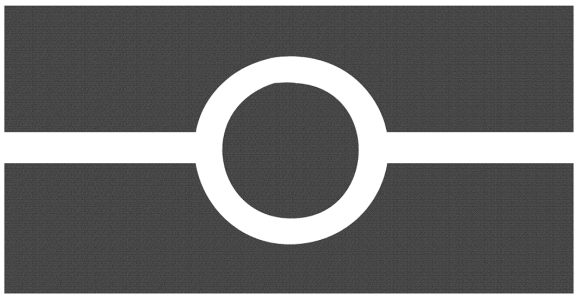
The Article 29 Data Protection Working Party of the EU member states found a paper on RFID PIA submitted by industry representatives in March 2010 to be inadequate (WP 175 of 13 July 2010). In particular, the committee noted that PIA should not merely describe the technology, but must identify its risks. Further, the paper did not discuss RFID tags carried by persons. Finally, the paper failed to analyse the deactivation of RFID tags at the point of sale, which is important from the perspective of data protection. Since then, the RFID PIA developed under the supervision of Global Standards One/Retail is in the process of being revised. Newer versions which however also require improvement were also submitted to the Article 29 Data Protection Working Party. These versions contain significant improvements over the first version. The industry has since submitted a final version, which the Article 29 Working Party assessed positively and officially endorsed. As a result, the RFID PIA will in future enable RFID to comply with high and uniform standards of data protection in all EU member states.

Box a for no. 5.9

RFID logo for products

Box b for no. 5.9

RFID logo for products



6 Telecommunications and postal services

6.1 Data retention: Quo vadis?

After the Federal Constitutional Court quashed the legal provisions on data retention for possible future use, the question now is what's next. The answer also depends on the evaluation of the EU directive on which the provisions were based.

The Federal Constitution Court decision

In my 22nd Annual Report (no. 3.2.1), I described the constitutional concerns regarding data retention for possible future use and reported on the constitutional complaint (for background information on data retention, see box a for no. 6.1). In its decision of 2 March 2010 (1 BvR 256/08), the Federal Constitutional Court found that the provisions on data retention violated the constitution and declared them null and void. I see this judgement as one in a series of fundamental decisions by the Federal

Constitutional Court on the population census and remote searches of computer hard drives which have reinforced data protection in Germany.

However, the fact that the court only found the legal provisions on data retention unconstitutional should not be overlooked; it also stated its view that the European directive on data retention could be implemented without violating the constitution, although such data retention would have to be subject to especially strict conditions due to its particularly invasive nature. The court listed four criteria:

- a high standard of data security,
- narrowly defined purpose for which the data may be used,
- sufficient transparency, and
- effective legal redress.

With regard to the data security requirements, the court incorporated my demands: Data retained for possible future use must be kept separate from other data stored for business purposes. The data must be encrypted and subject to a secure access regime, such as the principle of greater scrutiny. Finally, a revision-proof log of data retrievals is to be kept. Even if these rules cannot rule out every possibility of misuse, they could at least greatly reduce the risk.

The court found the legal provisions on the use of the data to be particularly inadequate, stating that they failed to restrict the use of data to an exhaustive catalogue of serious criminal offences. According to the court, due to the highly invasive nature of such use, using these data for purposes other than those law enforcement purposes to be specifically defined would be lawful only if absolutely essential to protect legal rights. The court also found that the requirement of restrictive conditions on use applied not only to the transmission of data to law enforcement authorities but also to the use of data already transmitted. These may be used only for the defined purpose, must be processed as quickly as possible and deleted immediately once they have served their purpose, according to the court.

The court also clarified that data collection and use must take place with the data subject’s knowledge and may be conducted covertly only in exceptional cases with a court order. The court also stated that an effective system of legal protection was needed to ensure that data are not transmitted from telecommunications operators to law enforcement authorities without a court order, and that effective legal protection proceedings ensure that the use of data is monitored after the fact.

The court's findings that preventive data collections in the absence of specific grounds may not exceed a certain limit should also be stressed (see box b for no. 6.1). Comprehensive monitoring without specific grounds for suspicion would contradict the constitutional identity of the Federal Republic of Germany, the court said.

I agree with the court's finding that IP addresses may be an appropriate way to identify Internet users on a large scale. But the court found that less stringent conditions apply to releasing the data of customers identified using IP addresses than to information about other telecommunications traffic data.

Freezing as an alternative

Even though the Federal Constitutional Court decision stopped the retention of telecommunications data in Germany for possible future use, this does not necessarily mean the end to all such data retention. As mentioned above, the court found that the legal provisions were unconstitutional, while indicating that the Data Retention Directive could be implemented in compliance with the constitution. As a result, the responsible Federal Ministry of Justice faces growing pressure to draft new legal provisions on data retention. Happily, the ministry has not yet bowed to this pressure.

I also believe that a hasty reintroduction of preventive data retention would be wrong. On the one hand, I have not seen convincing evidence that preventive data retention would in fact improve the clear-up rate for serious crimes to an extent that would justify this major infringement on the basic rights of all telecommunications users. The lack of empirical evidence is apparently not just a German issue: The European Commission postponed the assessment of the Data Retention Directive scheduled for 2010 until the first quarter of 2011 for lack of informative material (see below). On the other hand, it does seem plausible that certain crimes, especially those committed exclusively via the Internet, would be very difficult to solve without being able to trace dynamic IP addresses to perpetrators.

I have therefore advocated seeking a procedure which both allows effective prosecution and represents a data protection-compliant alternative to long-term preventive data retention without specific grounds for suspicion. In my view, the modified "quick-freeze" procedure I brought up in the public discussion some time ago would satisfy both conditions.

According to this model, at the order of the law enforcement authorities, telecommunications operators would have to retain, or "freeze", telecommunications data which might be needed to solve a crime and would otherwise be deleted, for a certain period of time. During this period of time, the law enforcement authorities could then get a court order requiring the telecommunications operators to give them the data. If a court order cannot be obtained within a certain period set by law, the “frozen” data would be deleted without being provided to the law enforcement authorities. A similar procedure has been used successfully in prosecuting copyright violations (see no. 4.8).

This model is problematic only when data are deleted immediately after the connection is terminated, as in the case of Internet access data of flat-rate customers. These data would have to be excepted from the regular deletion for a certain short period in order to be available to “freeze” (“quick freeze plus”). But putting this into action would require specifically assessing the degree to which the very limited buffering of data would help prevent or solve serious crimes and which specific data would be needed. I believe it goes without saying that this must be an absolutely restrictive selection and that the data must be subject to special security requirements, such as those defined by the Federal Constitutional Court for data security.

I believe that such a procedure could both serve the public interest in prosecuting crimes, on the one hand, and protect the confidentiality of telecommunications and the right to determine the use of one’s own data, on the other, to a degree acceptable to both sides.

A new direction from Brussels

There is yet another reason for not reintroducing legislation on preventive data retention: The European Commission is currently evaluating its Data Retention Directive and has announced that it will present the report originally scheduled for 2010 by the end of the first quarter of 2011. Even though it is unlikely according to current information that the entire directive will be repealed, as demanded in a resolution of the Conference of Data Protection Commissioners of the Federation and the *Länder* (see box c for no. 6.1), the Commission has signalled that the directive could be amended. For example, EU Commissioner Reding, who is responsible for data protection law, supports my "Quick-Freeze-Plus" proposal as a reasonable alternative to preventive data retention without specific grounds for suspicion. And Home Affairs Commissioner Malmström, who is responsible for the Data Retention Directive, hinted in a speech that the Commission is leaning towards making the

directive clearer especially with regard to data use and shortening data retention periods.

The Commission will decide after the above-mentioned evaluation process, to which I also contributed, has been completed. As part of a study by the Article 29 Working Party in 2009, I inspected several telecommunications operators in order to get a better idea of how preventive data retention is implemented in practice. The insights I gained from those inspections – and the significant shortcomings in implementation I found – were included in my comments to the Federal Constitutional Court and in a report of the Article 29 Working Party (WP 172 of 13 July 2010) which was provided to the Commission in the framework of the evaluation process.

Box a for no. 6.1

Background information on preventive data retention

Directive 2006/24/EC was adopted on 15 March 2006, requiring all EU member states to introduce preventive retention of telecommunications traffic data for the purpose of prosecuting serious crime (see 21st Annual Report, no. 10.1). In Germany, this directive was transposed into national law by means of the Telecommunications Interception and Other Undercover Investigation Measures Reform and Transposition of Directive 2006/24/EC Act on 1 January 2008. With this amendment, telecommunications operators were required to save the traffic data of their customers for six months and provide them to the prosecuting authorities, the police for preventive and official duties and to the intelligence services with the proper legal authorization.

Data to be retained include telephone connection data, such as the number of the caller and the number called, the exact time and length of a call; in the case of mobile telephone calls, the cell ID at the start of the call, the SIM card number and mobile handset identification number. From 1 January 2009, data generated from e-mail and Internet use also had to be retained, in particular IP and e-mail addresses.

With its decision of 2 March 2010, the Federal Constitutional Court found the legal provisions on preventive data retention unconstitutional and void. The Romanian constitutional court also found the national implementation of the directive on preventive data retention to be unconstitutional. A similar case is pending before the Hungarian constitutional court. The Irish High Court has also asked the European Court of Justice whether the directive violates the guaranteed fundamental rights of

the Community. In early 2009, the European Court of Justice found that in formal terms, the directive was enacted on the proper legal basis. The court deliberately did not comment on the legality of the directive's substance.

The Commission may have already amended the directive before the court makes a decision. The Commission's assessment is to be concluded by the end of the first quarter of 2011.

Box b for no. 6.1

Quotes from the Federal Constitutional Court decision on preventive data retention

"Retention cannot be justified in the abstract but only as far as it serves important, specifically defined purposes."

"The constitutionality of preventive retention without specific grounds for suspicion ... depends on [such retention] remaining an exception. Nor may it be used in conjunction with other available data to reconstruct virtually all the activities of individuals."

"Individuals' exercise of their freedom may not be recorded and registered in full. This is part of the constitutional identity of the Federal Republic of Germany. The Federal Republic must defend this identity in European and international contexts."

Box c on Section 6.1

Resolution of the 79th Conference of Data Protection Commissioners of the Federation and the *Länder* of 17–18 March 2010

No preventive data retention!

In its decision on preventive data retention of 2 March 2010 (1 BvR 256/08), the Federal Constitutional Court described the preventive retention of telecommunications data without specific grounds for suspicion as an "especially serious intrusion on a scale previously unknown in the legal system". Because such retention makes it possible to create informative personality and movement profiles of virtually everyone in Germany, the Conference of Data Protection Commissioners of the Federation and the *Länder* categorically reject preventive data retention. The ban

on comprehensively collecting data on individuals is part of the constitutional identity of the Federal Republic of Germany, which is to be defended also in European and international contexts. The Conference therefore calls on the Federal Government to advocate the repeal of European Directive 2006/24/EC.

Further, the Federal Constitutional Court stresses that individuals' exercise of their freedom may not be recorded and registered in full. The decision therefore has implications for other areas as well, such as the controversial retention of airline passenger data and the design of road toll systems. And the central ELENA database will have to be examined. When considering new retention obligations or authorizations with regard to the totality of various data collections, legislators are called on to show greater restraint.

6.2 They know where you are: The growth of location services

More and more mobile devices make it possible to locate their owners with increasing precision.

Mobile telephones and other mobile end-user devices function only when connected to mobile networks. Location data, known at least to network operators, are generated in this way as by-products. But third parties are also interested in these data: providers of location-based services, advertisers and emergency services.

More and more mobile devices contain built-in technology which uses satellites and identifying data from wireless local area networks (WLAN) (see no. 4.1.2) to locate the device within a few metres – even indoors. The more precise the location data, the more they interest potential users, and the more important it is to protect data subjects against location without their knowledge. Even when the location of mobile devices is concerned, the legal assessment of location mechanisms is complicated – reason enough to update my previous reporting on this issue (see most recently 22nd Annual Report, no. 7.7).

Mobile phone tracking under the Telecommunications Act (TKG)

In my 22nd Annual Report, I reported on draft legislation to amend the Telecommunications Act, which entered into force in August 2009 (Federal Law Gazette I 2009, p. 2409). The amended legislation is intended to prevent the risk of misuse for classic mobile phone tracking carried out by network operators. The most important new features were that written permission from the subscriber was required

for tracking by third parties, and that subscribers had to be informed by SMS after being located five times.

However, ambiguities and possibilities for getting around the provisions were revealed during their implementation. For example, the law does not make entirely clear who is responsible for what. The mobile phone service contract can be with a service provider, the mobile phone service is provided by a network operator, and a tracking service provider operates the tracking platform and makes contracts for tracking services. The subscriber is only aware of the phone service provider, which actually has nothing to do with the tracking process.

For practical reasons among others, the Federal Network Agency (BNetzA) regards providers of tracking services as being obligated to have written subscriber consent. In order to deal with the risk of misuse, according to the Federal Network Agency tracking service providers must take appropriate measures to ensure effective consent. Such measures could include requiring the subscriber to submit, along with written consent, a statement confirming that she is the contracting partner for the mobile telephone number given.

I doubt whether this will be effective in stopping misuse. The SMS required by the Telecommunications Act – theoretically to be sent by the phone service provider, which is not aware of the tracking – applies only when no objection has been made to SMS notifications. The option to forgo notification allowed by the Act could well open the door to misuse in some cases.

Another problem is subscribers tracking their own mobile phones. Under Section 98 of the Act, a subscriber who wishes to track her own mobile must neither submit written consent nor receive an SMS notification. The Act regards subscribers with multiple SIM cards, such as a partner card for a spouse or for an employer-supplied mobile phone, wanting to track these phones as also tracking their own mobiles, even though the purpose would really be to track the location of another person. In this case, no written consent is needed and no SMS notification needs to be sent, thus facilitating misuse.

In view of these risks, I am glad to see that many providers always require consent via SMS from the mobile phone to be tracked before enabling tracking.

The Federal Ministry of Economics and Technology has reacted to these problems and opened a discussion of Section 98 as part of the current process of amending

the Act. At my suggestion, according to the version at the time this report went to press, an SMS notification must always be sent to the end-user device unless the location data are to be displayed only on that device. This kind of tracking would apply to services showing nearby restaurants, for example. I hope that the proposed provision will be adopted as soon as possible in order to reduce the possibility of misuse in connection with tracking services.

Tracking smartphones

While any mobile phone can be tracked via the network operator, this option is seldom used. Tracking smartphones, on the other hand, has become routine. Owning one of these handheld computers with telephone, camera, WLAN and GPS functions and a flat-rate plan is almost de rigueur in certain circles (see also no. 5.11). And they can be tracked using GPS, WLAN and cell data without the participation of the network operator. Data sent wirelessly are typically transmitted via the Internet to a provider – most of them American – which determines the phone's location. In addition to GPS data, databases with readings from WLAN stations and base stations are also used, so that phones can be located even without GPS reception. In return, the data transmitted by smartphones, combined with geodata gathered by special vehicles (see no. 4.1), provide the necessary informational basis. In this way, one can view a map of the local area, assign a geolocation tag to a photo, show one's own position to friends in a social network, or view advertising for local businesses.

These location data are covered not by the Telecommunications Act but by the Telemedia Act, as the telecommunications operator does not provide the location service itself. As a result, the data protection supervisory authorities of the *Länder* are responsible. Because these services are offered in many cases by American companies, European supervisory authorities unfortunately have little influence on how the location data are generated and used.

Very few users understand the processes at work when they use a smartphone to look for nearby restaurants. Surprising details emerged from a U.S. company's testimony to Congress in summer 2010 regarding the tracking functions of its devices: When tracking is activated, devices send data to the company under an alias and, if the user has not opted out of local advertising and the tracking function is not deactivated, the user's location is identified to the closest postal code and stored. Applications that can be downloaded onto a device are also subject to rules, for example that the user must provide consent and the location information is essential to the application. Even though the testimony clarifies some points, many questions remain unresolved upon closer inspection, such as how long data are retained. And

opinions may differ as to whether data are anonymous or aliased, or whether they can identify specific persons.
These data are usually transmitted only after a user has agreed to the terms of use. But it is doubtful whether the few users who actually read these terms understand their full implications. Here I must call on every user to imagine the possible implications before providing consent or activating the tracking function and to use proper caution.

Emergency call tracking
Following enactment of the emergency call regulations on 6 March 2009 (Federal Law Gazette I, p. 481), I expect the Technical Guideline on Emergency Calls (TR Notruf) to be ready in early 2011. The initial draft did not resolve the problems I pointed out. In particular, when multiple network operators are involved, such as VoIP and Internet providers, they should be required to cooperate in tracking. The emergency call regulations state that appropriate measures are to be taken to protect the technical interfaces against misuse. The draft Technical Guideline does not mention how this is to be carried out, however. I do not foresee a satisfactory technical solution at this point. Because VoIP calls must be located to determine which emergency response centre has jurisdiction, a solution must be found to protect user's IP addresses from being localized through misuse of standardized emergency interfaces by unauthorized third parties.

The Technical Guideline should contain clearer rules on locating mobile calls to emergency response centres. Currently, a mobile call can be located as needed by the emergency call tracking system initiated by the Björn Steiger Stiftung and now operated by the Allianz OrtungsServices GmbH (AOS). In this case, the emergency response centre asks for oral consent. As currently amended, Section 98 of the Telecommunications Act would require written consent, which would be impractical in emergencies. It was therefore suggested that locating should be conducted formally on the basis of Section 108 of the Act, with the AOS serving as data processor for the network operator. This would meet the formal requirement that the network operator transmits the caller's location data to the emergency response centre. This solution would comply with the law until the Technical Guideline must be applied. At the time this report went to press, however, not all the necessary contracts had been signed.

6.5 Deep Packet Inspection: Are operators allowed to inspect communication content?

Telecommunications service providers may inspect the content of communications only in exceptional cases to conduct repairs. It is unlawful to analyse content using Deep Packet Inspection or to store content in log files on proxy servers.

When inspecting a wireless service provider, I found that data (web pages) in mobile Internet use were altered and the alteration was documented within a log file. The content was altered by a proxy server (see box a for no. 6.5) to store information from the data packet in addition to the header content within the log files. A similar procedure is possible using Deep Packet Inspection (see box a for no. 6.5), which in some cases is available to network operators.

Providers usually refer to Section 100 (1) of the Telecommunications Act, which states that they may collect and use customers' inventory and traffic data to repair faults. In addition to the usual traffic data, the recorded data include the URL visited, the HTML status code contained in the response and the type of browser and are (sometimes) kept in anonymous form. Before the information is processed, the URL is reduced to the domain name. So it is conceivable that the data recorded are used not only to repair faults, but also for further – typically statistical – analysis of user behaviour, for example to measure mobile Internet traffic. This information can also be used to analyse the frequency of visits to a certain website and to create and/or evaluate marketing strategies. Closer inspection of this technology and its application raises the question whether analysing the packets violates the confidentiality of telecommunications, apart from the question of regulating data streams.

From a technical perspective, access to the Internet and the transmission of data on the Internet is designed as digital packet communication: Data to be transmitted (e.g. websites, e-mails, etc.) are broken down into small "parts", combined into packets and sent across data lines between the various Internet routers, for example from the provider via a DSL connection to a home computer or via a wireless connection to a smartphone. Data packets are generally divided into the header and the content. The header contains the information necessary to direct and process the data packets. The header data and content of packets vary depending on the protocol used; different protocols may also be used as a hierarchical data structure (see box b for no. 6.5). This structure can result in a large accumulation of data, of which only a small proportion is necessary for technical processing by the access provider. Unlike classic telephony, data packets are (usually) transmitted without a direct connection to their destination. With telephone calls, the telephone number determines the

destination and allows a dedicated communication channel; by contrast, data packets must be analysed constantly and further transmitted on the Internet using their headers. This makes it increasingly difficult to distinguish a single piece of data and classify it as traffic, usage or content data (see 22nd Annual Report, box for no. 7.8).

Whereas there is no doubt that a telephone number constitutes traffic data, the classification of a URL (of a requested website) contained within a complex set of protocols is subject to debate. Here it is essential to consider the specific case: For example, if a server hosts several websites but has only one IP address, the content provider (here: the hosting service provider) must analyse the URL to direct the request to the right website. By contrast, the content does not need to be analysed to send the message, because the destination is clear from the IP address (or the domain). When proxy servers are used, for example for mobile Internet access, the distinction between access and content provider is somewhat more complicated. Proxy servers are able to communicate with and influence the requested URL themselves, instead of sending the packets on sight unseen. Some proxy servers not only alter the appearance of a website, but may also re-format multimedia content (such as video). This process is comparable to the alteration of language coding during a mobile telephone call. Analysing the packet content is analogous to analysing the basic language frequency found in language coding which makes it possible to document whether the caller is male or female.

The content of the data packets is thus not only transmitted, but also altered. To simply transmit data via a proxy server, it would suffice to analyse the destination and/or sender data in the packet header. Regardless of whether traffic or content data are concerned, there is no legal basis for altering the data. The same applies to other forms of Deep Packet Inspection, which allow transmitted or temporarily stored content to be analysed. The use of this technology by Internet access providers and providers of proxy servers usually violates the confidentiality of telecommunications, except to repair a specific fault or to automatically protect against malware, and if the analysis is limited to address information.

I will therefore monitor service providers for compliance with the law.

Box a for no. 6.5

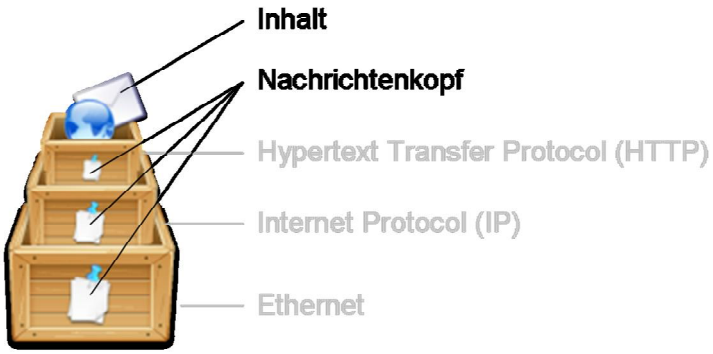
In network technology, **Deep Packet Inspection** (DPI) refers to a process which makes it possible to monitor data packets and analyse them at various levels. Both the header and the content of the communication may be analysed. Access and

content providers use this technology to screen for viruses, spam and certain protocols, such as Voice over IP (VoIP) or instant messaging within data packets.

For wireless Internet, data packets are sent via special proxy servers which adjust the content of websites visited to display them on (simple) mobile telephones and to send them through mobile networks faster. Proxy servers are used with high-performance devices because the data must be altered during transmission via the wireless network, where delays and packet loss rates are much higher than in DSL networks. When using simple mobile telephones, it also makes sense to adjust the way websites are displayed. The decisive criterion here is not only the smaller processing capacity of mobile telephones, but also their smaller screens.

Box b for no. 6.5

Nested, hierarchical data structure of common communication protocols



The graphic shows the nested protocol hierarchy needed to view a website on a PC, for example. Each protocol level creates a data packet out of the available information, assigns it a header (similar to an address label) and forwards the data to the next-lowest level. In this example, the ethernet packet represents the “shipping container” for transmission over the network.

6.7 The underestimated risk of interception

It is becoming ever easier to intercept telecommunications content. Not only wireless and mobile communications media are affected. Existing protective mechanisms must be applied – anyone who fails to do so is acting irresponsibly.

A corporate data protection official informed me of a case of interception in cable communications: A local telecommunications company offered a telephone and

Internet package over its own cable network. Service contracts were initially made on a trial basis. The problem was that telephone calls during the trial period were not encrypted and were able to be intercepted for at least three months. According to the public prosecutor's investigation, interception was possible using simple hardware (e.g. PC with DVB-C card) and software available on the Internet. It was possible to receive the unencrypted telephone calls at first on the entire network and then in larger segments.

According to Section 109 (1) of the Telecommunications Act, every service provider must take appropriate technical or other measures to protect the confidentiality of telecommunications and personal data and to protection telecommunications and data processing systems against unauthorized access. In this specific trial, customers were not informed in language understandable to all about the special risks of network security, in violation of Section 93(2) of the Telecommunications Act. The telecommunications company has since improved its telephone and Internet service and has begun regular, encrypted operations.

A petitioner wrote me that his DSL connection (see box for no. 6.7) was being slowed by "foreign" data. As he explained it, the problem was that the channel for data from the DSL provider to the client (downstream) was sending so much data even when not in use that he was unable to access the Internet or make telephone calls. His analysis of the incoming data showed that they were intended for a different customer or customers of the DSL provider and were addressed accordingly. According to the petitioner, while analysing the data, he was able to decode the content of the data packets and listen in on telephone conversations (VoIP), for example. An intensive investigation revealed that both an inadequate (or very open) hardware configuration in the past (unintentionally) led to unauthorized access, and that hardware defects displayed these and similar symptoms.

Already in 2009 it was found that telephone calls made using Digital Enhanced Cordless Communications (DECT) could be intercepted with little expense or specialized knowledge, because the cost of hardware needed for interception has fallen and because most makers of current DECT products fail to use the optional DECT-standardized encryption, despite knowing better. Users are not able to tell whether the device they use takes advantage of the DECT encryption options or whether the data are transmitted unencrypted.

The wireless situation is equally problematic. Although encryption is being used on a large scale for wireless transmissions (here: GSM), the algorithm used is so old that it

no longer meets current requirements for protection against interception. In December 2009, computer experts presented an inexpensive way to decode mobile telephone calls in less than 20 minutes.

Overall, I view the current situation regarding the risk of interception with concern, especially since the rapid development of technical possibilities for communications surveillance gives reason to fear that worse is on the way. The growing lack of security due to the widespread availability of technologies to listen in on and decode wireless communication could be easily countered using up-to-date encryption algorithms. I believe it is irresponsible that, for purely economic reasons, most makers of wireless telephones market their devices without the encryption found in the DECT standard without making this apparent. It should also be remembered that Section 109 (1) of the Telecommunications Act requires all service providers to protect the security of content data by ensuring that hardware is correctly configured and functions properly.

Box for no. 6.7

In a DSL connection, subscriber lines of multiple customers run to the provider's central office, where voice signals are split from data signals. The Digital Subscriber Line Access Multiplexer (DSLAM) connects multiple customer DSL lines to the provider's network. The next network component is the DSL Access Concentrator (DSL-AC), which connects to the Internet.
In a "classic" DSL infrastructure, customer data from the DSL modem are aggregated and transferred via Asynchronous Transfer Mode (ATM) to the DSL-AC in a point-to-point connection. The ATM function principle uses a private (virtual) channel to protect the data from being "seen" by other customers.
Next-Generation Networks (NGN), which are often used by providers which do not have their own lines, are often run using the ethernet protocol regardless of the network infrastructure. Unlike the classic networks, the ATM structure is already dissolved in the DSLAM and the data are transferred to the DSL-AC as ethernet packets. The packets of multiple customers are transferred via the same connection, which makes it difficult technically to separate customers.

6.8 The E-Postbrief is on its way. Will it arrive safely?

Deutsche Post AG carried out most of my design and data protection recommendations into account.

Since summer 2010 Deutsche Post AG has been offering a new form of mail delivery, called “E-Postbrief”. The company informed me about the new service before it was introduced. The E-Postbrief offers the option to deliver letters in conventional, paper-based form or in electronic form. To participate, whether as sender or recipient, requires individual registration. There are two channels for delivery: the fully electronic channel, in which an electronic message from the sender is transmitted directly to the recipient; and the channel in which only the sender, not the recipient, is a registered E-Postbrief participant. In the latter case, the sender’s electronic message is printed out by Deutsche Post AG, put in an envelope, addressed and delivered to the recipient like a conventional letter (see box for no. 6.8).

For the fully electronic channel (both sender and recipient are registered participants), complete confidentiality is not yet guaranteed, as the channel does not use end-to-end encryption. For this reason, as in the case of De-Mail (see no. 3.3), senders must take additional measures on their own to ensure the confidentiality of especially sensitive data (such as health data), for example by enclosing these data in an encrypted attachment. In the case of electronic messages printed out for conventional delivery (“hybrid letter”), confidentiality is to be guaranteed by the fact that staff entrusted with printing out the messages who violate the privacy of posts and telecommunications (Art. 10 Basic Law) are subject to criminal prosecution.

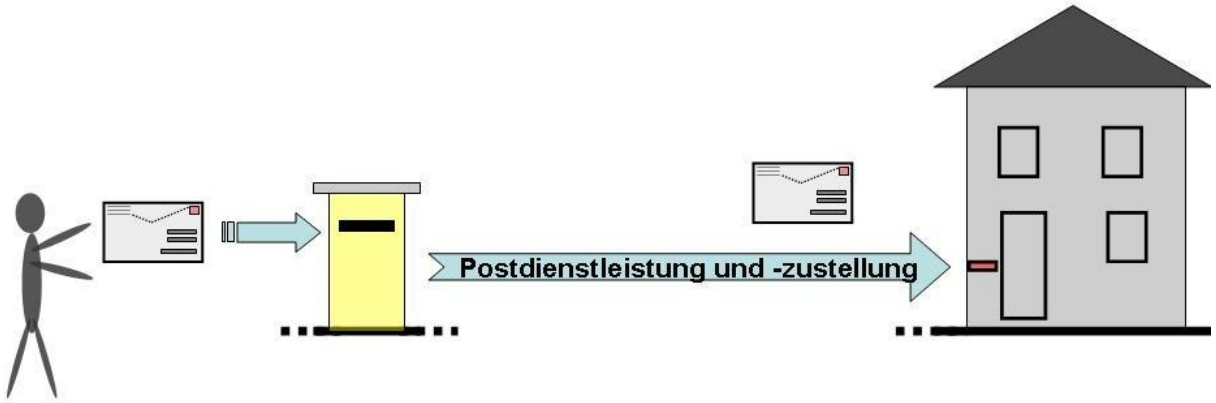
In late October 2010, I visited the computing centre which provides the applications and digital processing and a printing centre which will send hybrid letters. Neither visit revealed any problems in terms of data protection law. The printing centre has long been responsible for printing out other documents with sometimes sensitive contents, such as invoices and account statements, on behalf of numerous companies.

So far, I have only received a few complaints about the E-Postbrief. Most of them have to do with the registration process (mobile telephone number required for the TAN procedure) and with the Deutsche Post AG printing out the E-Postbrief when conventional delivery is the only option. Among other things, concern focused on whether the privacy of posts was ensured. Parties to the delivery contract are only the sender and Deutsche Post AG, so that recipients have no influence on the delivery form. Because letters are printed under the terms of a contract with Deutsche Post AG, from the perspective of data protection law it remains responsible for upholding the privacy of posts.

Box for no. 6.8

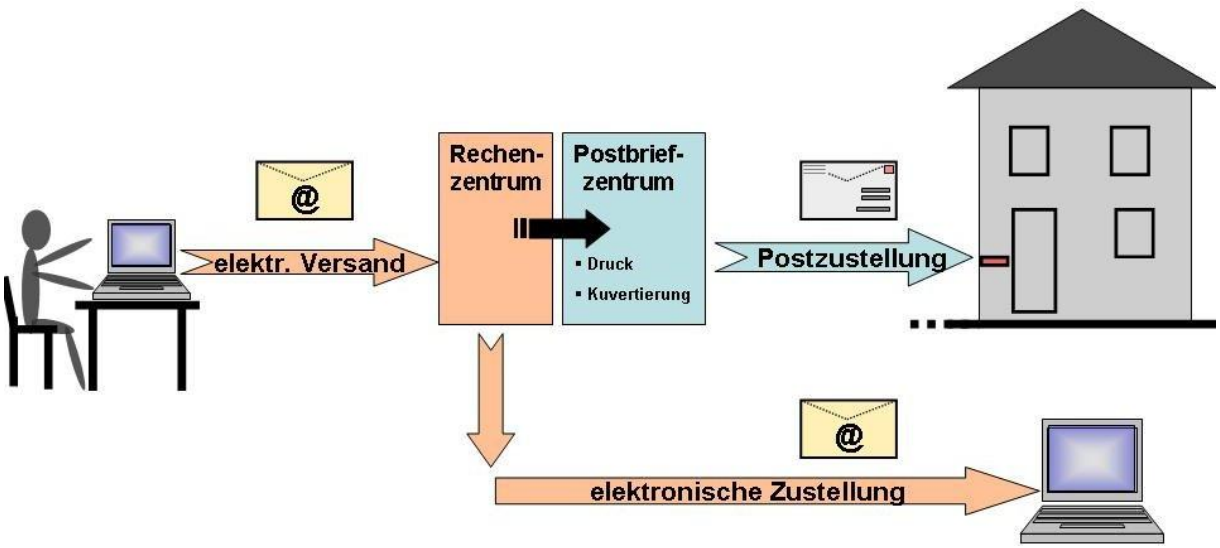
The E-Postbrief in comparison with conventional postal delivery:

Conventional letter:



Sender **Recipient**

E-Postbrief:



Unlike a conventional letter, the E-Postbrief is produced and sent electronically. If the recipient has registered with the service, the message will be delivered in electronic form. If the recipient is not registered, the message is printed, put in an envelope, addressed and delivered like a conventional letter (“hybrid letter”).

6.9 Due diligence requirements of telecommunications companies vis-à-vis their customers

In a decision by the Bonn Regional Court of 1 June 2010 (7 O 470/09), a telecommunications company was required to inform its customers as quickly as possible about any unusually high charges. However, the question remains as to how this is to be done in compliance with data protection law.

A customer sued her telecommunications company for reimbursement of excessive charges. There was no question that the charges were actually incurred, because the customer used an Internet rate charged by the minute. But the router provided by her telecommunications company was configured to maintain a connection, even when the customer was not using the Internet. The resulting costs amounted to more than €5,000 in five months. The court found for the customer, arguing that, due to the contract for a continuing obligation, the telecommunications provider had a special obligation to provide for the customer's welfare, which required the provider to respond to unusual customer behaviour within a few days.

However, the court did not address the question how this obligation was to be met in practice in compliance with the law. The Telecommunications Act (TKG) clearly defines the boundaries within which telecommunications providers may use the inventory and traffic data of their customers. Permanent monitoring of traffic data, as this case would seem to require, would violate the Act. Section 100 (3) of the Act allowing traffic data to be processed in order to detect misuse of telecommunications networks does not apply here, because the reason for the high charges was not misuse but an improperly installed router.

In my view, usage could be monitored only via the billing data, which are generated under the terms of the contract and thus may be used as inventory data needed to provide telecommunications services, in line with Section 95 (1) of the Act. Should a telecommunications provider find unusual customer behaviour when checking the billing data, the provider may inform the customer. However, the provider may not take any measures other than informing the customer, in particular viewing traffic data to determine the source of the anomaly, without the customer's explicit permission. Telecommunications providers must therefore live with the sword of Damocles in the form of such court judgements which are nearly impossible to carry out in compliance with data protection law.

6.10 Re-assignment of e-mail addresses

When e-mail addresses are re-assigned too quickly, messages may be misdirected. I believe a waiting period of at least three months is appropriate.

Many people wrote to my office to complain that after they had terminated their contract with an e-mail provider, their old e-mail address was assigned to a new customer within such a short time that messages were sent to the wrong recipient. Senders were usually not aware that their messages were not going to the right person, due to the lack of direct contact to the recipient.

Every e-mail user is responsible for informing their contacts of e-mail address changes. Nonetheless, I can understand when this is not possible in every case. I therefore agree with the recommendation made at the 47th Meeting of the International Working Group on Data Protection in Telecommunications: E-mail addresses should be reassigned after a waiting period of three months. I have recommended to German providers of e-mail addresses that they follow this recommendation.

7 Internal security

7.1 Federal security architecture

7.1.2 The counter-terrorism database of the federal intelligence services

Data processing by the domestic and foreign intelligence services in the counter-terrorism database displays serious shortcomings.

After checking data processing by the Federal Criminal Police Office (BKA) in the counter-terrorism database (see 22nd Annual Report, no. 4.2.2.2), I concentrated during this reporting period on checking the data processing by the Federal Office for the Protection of the Constitution (BfV) and the Federal Intelligence Service (BND). In the process, I found serious shortcomings in some cases.

Data from a source file maintained by the BfV is automatically transferred to the counter-terrorism database. This leads to problems with the transfer of extended basic data: Certain data stored lawfully in the source file may not be added to the counter-terrorism database under the more restrictive provisions of the Act on Setting

up a Counter-Terrorism Database (ATDG). Here, more careful selection is needed before data are transferred to the counter-terrorism database. I also found that data records which were to be deleted from the source file were retained in the counter-terrorism database, and free-text fields contained remarks which were not permitted. Happily, the BfV is aware of the problems and has agreed not only to remedy the shortcomings in the system, but also to provide special training to ensure that information is added to the counter-terrorism database properly.

In violation of the ATDG, the BfV added all the data collected from covert telecommunications surveillance to the counter-terrorism database without the required special marking. As a result, the other agencies with access to the database used these data without the special marking. Without such marking, no one can tell that these data are under special legal protection and may be processed only under special conditions. The BfV system which transfers data from source files to the counter-terrorism database made no provision for such marking. This problem affected much of the data. At my request, the BfV agreed to mark the relevant data as required by law and to ensure that all recipients of the data were informed of their requirement to mark the data accordingly. I therefore did not make a formal complaint. I will check to make sure the BfV carries out these things as agreed.

Another unresolved data protection problem is deciding when a contact person should be classified as “dolos” as defined in the ATDG: “Dolos" means that there are concrete indications that the persons concerned are aware of the planning or commission of a terrorist offence or of the commission, support or preparation of unlawful acts of violence as defined by the ATDG. Significantly more data may be collected on persons classified as “dolos” and their right to determine the use of their own data may be further encroached upon. Contrary to the BfV’s interpretation, the experience of intelligence agencies is not sufficient to establish this status. Because storing data in the counter-terrorism database represents a serious intrusion upon basic rights, the person in question must be connected to a specific act which they knowingly support.

At the time this report went to print, the assessment of material added by the BND to the database had not yet been completed. I will report on the results in the next Annual Report.

7.1.3 Logging conducted by the security authorities

Growing information networks between the security authorities and the creation of large-scale databases by federal police forces and intelligence services require new avenues for data protection which meet the needs of the various agencies. One option is to make greater use of the protocol data generated by database systems operations. However, this will require a complete log of all database transactions for the purpose of data protection (see above, no. 5.7).

7.1.7 Police investigation using social media

Investigating via the Internet has become a major part of police work (see 18th Annual Report, no. 11.8; 21st Annual Report, no. 5.1.3). This includes increasing research in social media.

The BKA also uses social media (see above, no. 4.5) and other open sources for clarification in investigations and to fulfil its tasks as a central agency under Section 2 of the Federal Criminal Police Office Act (BKA Act, BKAG). The aim is to detect when specific offences have been committed and to report these to the law enforcement authorities with jurisdiction. With reference to the Federal Constitutional Court decision of 27 February 2008 on remote searching of computer hard drives (1 BvR 370/07; see also 22nd Annual Report, no. 4.1.1), the BKA stresses that, as a rule, investigations conducted via the Internet do not intrude on basic rights. If such research via social media does intrude on basic rights, according to the BKA, Sections 161 and 163 of the Code of Criminal Procedure or Section 7 (1) and (2) of the BKA Act apply.
This raises the same issue as the activity of agencies participating in the Joint Internet Surveillance Centre (see above, no. 4.9). The determining factor is the stage at which police use of the Internet exploits the legitimate trust of data subjects in their communication partners. That issue notwithstanding, the Federal Constitutional Court decision referred to above stated that the right to determine the use of one's own data is infringed on whenever data collected on the Internet are purposely compiled, stored and analysed. This is the case when the BKA researches in social media as part of criminal investigations or for the purpose of analysis as part of its tasks as a central agency.
I doubt whether the provisions cited by the BKA can justify the infringement on the right of data subjects to control the use of their own data in the case of investigations using social media. According to the Federal Constitutional Court decision of 15 December 1983 on the population census, any restrictions of this basic right require a legal basis clearly stipulating the conditions and extent of these restrictions in a way

apparent to data subjects. The generally worded provisions of Sections 161 and 163 of the Code of Criminal Procedure and Section 7 (1) and (2) of the BKA Act do not meet these requirements. In view of the legal uncertainty (noted not only by me) concerning the stage at which police research on the Internet constitutes an infringement of basic rights, I believe the content and limits of such authority should be governed by specific legislation.

7.2 Federal Criminal Police Office

During the reporting period, my work focused on assisting with efforts concerning the statutory instrument in accordance with Section 7 (6) of the BKA Act (see no. 7.2.1 below), checking the BKA's data processing of state security files for data protection compliance (see no. 7.2.2 below) and its involvement in background checks for accreditation for major events (see no. 7.2.3 below).

7.2.1 Very late: A statutory instrument on the types of data which the BKA as central agency may store

Last summer, the Federal Ministry of the Interior produced a catalogue of all the types of data which the BKA may store in its function as central agency. By doing so, the ministry met a demand I had long insisted on - though only under pressure from the courts.

My recent annual reports have repeatedly noted: “Still no statutory instrument in accordance with Section 7 (6) of the BKA Act” (see 22nd Annual Report, no. 4.3.2.3). That has now changed: On 9 June 2010, the Statutory Instrument on the Types of Data which may be stored under Sections 8 and 9 of the BKA Act entered into force, conclusively determining which kinds of data the BKA may store in databases in its role as central agency (Federal Law Gazette I, p. 716). This catalogue includes less critical types of data, such as name and place of birth, as well as more sensitive information, such as religious affiliation, bank accounts, whether there is an entry in the DNA database, and notes such as “leftist motivated offender”.

I have called for such a statutory instrument for years, most recently in a joint resolution of the 77th Conference of Data Protection Commissioners of the Federation and the *Länder* of 26-27 March 2009 (see box for no. 7.2.1). The BKA Act includes the obligation to enact such a statutory instrument – for good reason: This is the only way to give the Bundesrat a say on which data the BKA may store as central agency, and the only way to create appropriate transparency.

The Federal Ministry of the Interior resisted these arguments for years, until a decision by the Lüneburg Higher Administrative Court forced it to reconsider. The court in Lower Saxony found that storing data in the joint federal–state hooligan data file was unlawful in the absence of such a statutory instrument (decision of 16 December 2008, 11 LC 228/08). The decision also put into question a large proportion of the BKA's data processing, because if Section 7 (6) of the BKA Act requires a legal basis, as the court found, then this applies as well to all other databases managed by the BKA as central agency. Without a statutory instrument, all these databases would run the risk of being declared unlawful.

The Federal Ministry of the Interior just managed to avoid that situation, as the statutory instrument went into effect on the very same day that the Federal Administrative Court ruled on the appeal in the above-mentioned case. Although the Federal Administrative Court found the hooligan data file lawful for that reason, it left no doubt that it would have agreed with the Lüneburg Higher Administrative Court, stating that Section 7 (6) of the BKA Act did not simply allow a statutory instrument but rather strictly required one (decision of 9 June 2010, 6 C 5.09).

The new statutory instrument does not provide a legal basis for collecting or processing data; the aim was not to cover more data or new types of data, but to provide a lawful basis for storing the existing data. During the proceedings, I successfully insisted on including in the statutory instrument a conclusive list of all types of data allowed in the BKA databases; as a result, the BKA may not include any other types of data.

During the interministerial consultations, it was agreed that the statutory instrument should not simply be a single long list of data types, but should link these to the different types of databases. This plan was carried out, making the text of the statutory instrument extremely complicated.

Unfortunately, the opportunity to reduce the types of stored data to the necessary minimum was missed. The provisions of the statutory instrument used the fullest extent of the legal framework allowed by Sections 8 and 9 of the BKA Act, and my call to limit the data stored to basic data on persons in the database went unheeded. Nor was my suggestion to use the statutory instrument to further clarify the text of Section 8 (5) of the Act on "other persons" acted on.

Box for no. 7.2.1

Resolution of the 77th Conference of Data Protection Commissioners of the Federation and the *Länder* of 26–27 March 2009 in Berlin

There is no legal basis for data processing in INPOL by the police

The federal and *Länder* police forces may lawfully store data in the INPOL police information system only when a statutory instrument in accordance with Section 7 (6) of the Federal Criminal Police Office Act specifies the type of data which may be stored in this database. No such statutory instrument exists. In its decision of 16 December 2008 (file reference 11 LC 229/08), the Lower Saxony Higher Administrative Court underscored this with regard to the joint hooligan data file. The decision is not only relevant for the lawfulness of the hooligan data file, but also has ramifications for all networked databases maintained as part of the INPOL police information system.

The court's decision confirms the position of the federal and *Länder* data protection commissioners. The relevant provisions do not support the Federal Ministry of the Interior's argument that the statutory instrument is not a prerequisite for processing the data in the networked databases.

Without such a statutory instrument, all data processing by the police in the networked databases is in violation of the law. The federal and *Länder* data protection commissioners call on the Federal Ministry of the Interior and the *Länder* governments to immediately take the necessary action and examine data processing by the police.

7.2.2 Politically motivated crime: The BKA's IGAST database

The BKA's data storage practices in its IGAST database, which is used to send lists of anti-globalization protesters abroad in advance of relevant events, are cause for concern.

It has become standard practice among security authorities in different countries to exchange information on potentially violent demonstrators across international borders in advance of major political events, such as the NATO summit in Strasbourg and Kehl and the world climate conference in Copenhagen. The Federal Government's responses to enquiries from members of parliament on this issue have failed to resolve all my questions. I therefore checked on the BKA's data processing practices with regard to what it calls politically motivated crime. I focused on the BKA database on violent troublemakers who are active internationally (IGAST), the

successor to the Global database which has since been erased (see 20th Annual Report, no. 5.2.5.1).

The IGAST database has achieved some notoriety as the basis for a list of “violent troublemakers” who are opposed to globalization. The BKA sends this list to the police in the country hosting an event if violent demonstrations are anticipated. The recipients are instructed to destroy the data sent them no more than four weeks after the event. All the personal data transmitted in this context are covered by a data protection clause stating among other things that the data are subject to restrictions on use. Data are transmitted only if the receiving country has demonstrated an appropriate level of data protection.
The subject of my data protection concerns are not this practice of data transmission, however, but rather the structure of the IGAST database and the way it is managed: The persons included in the database are divided into two categories, although the order opening a file, which is in my possession, makes no reference to such division. One category includes persons considered to belong to the “hard core” of violent troublemakers, who are put on the list referred to above as necessary; the other category is made up of persons who are included in the database only to determine at a later date whether to add them to this list or delete their files within the data retention period. So the database contains files on accused persons, suspects and other persons as referred to in Section 8 of the BKA Act, but contrary to the order opening the file, it does not contain information on innocent persons, such as witnesses or contacts. Nor does the order opening a file specify the conditions for data transmission, and thus fails to provide the specification required by law.
I also did not get a sense that the BKA had a clear definition of who constitutes a “violent troublemaker active internationally”, especially with regard to those persons with files in the database who are not considered part of the “hard core” of violent troublemakers. The factual basis on which the BKA must make this decision also often seemed uncertain, especially since the BKA has to rely on sometimes very sketchy information from abroad or from the *Länder*. Nonetheless, the BKA is responsible under data protection law for the data stored in the IGAST database. As I told the BKA, I see no justification for storing data in certain cases, such as when demonstrators were included in the database for having blocked streets as part of a human chain or of the “Naked Block”. Regardless of whether the actions of protesters can be considered violence in terms of criminal law, their data should be stored in the database only when the form of political protest chosen is obviously intended to injure humans or cause significant property damage. This is the only way to ensure that even provocative forms of political protest continue to be allowed. Even if the names of persons in these cases are not sent abroad, the fact that they are stored in

the IGAST database alone constitutes intrusion on their right to control their personal information.

The BKA has agreed to review its data storage practices. No comments were available by the time this report went to press.

7.3 Federal Police

During the reporting period, I focused on issues of technological data protection: participating in the discussion of introducing full-body scanners at airports and the related Federal Police research project (see no. 7.3.1 below); monitoring the pilot project on the easyPass biometric border control procedure (see no. 7.3.2 below) and the introduction of electronic criminal records for the Federal Police (see no. 7.3.3 below).

7.3.1 Full-body scanners at German airports: Progress and problems

Full-body scanners are being tested at German airports for the first time. It appears that my calls for comprehensive privacy protection have so far been taken into account.

Many of the measures taken to counter terrorist and criminal threats pose a dilemma for data protection, among other things: How far may privacy rights be encroached upon to counter these threats or at least minimize the risks? In many cases, one must choose between alternatives which may each have troubling implications. This is especially true for aviation security, which has been the repeated target of terrorist activity.

Following the attempted bombing on board a jet bound for Detroit on Christmas Day 2009, a discussion on the utility and risk of introducing body scanners at German airports began also in Germany. I received a wide variety of e-mails on this topic. Some showed little understanding for data protection concerns, while many others were worried about protecting their privacy. They feared that their sense of modesty would be violated or that this new form of imaging would reveal their medical conditions or unusual features, if not to the public then to strangers, especially as images of nude bodies produced by full-body scanners were then circulating in the media.

To focus the public debate on the facts and to clarify which boundaries should not be crossed in the search for greater security, I formulated data protection requirements to be met in order for body scanners to be introduced. To this end, the data protection commissioners of the *Länder* and I drew up a resolution at the 79th Data Protection Conference on 17-18 March 2010 (see box for no. 7.3.1).

In the resolution, we stated that no body scanners should be used unless there was evidence that they increased security; that the data generated should not be stored; and that the dignity of the individual should be fully protected by not displaying body contours, sexual characteristics or medical aids (such as adult diapers or colostomy bags) to screening staff.

Measured against these criteria, I find the scanners currently being tested by the Federal Ministry of the Interior at Hamburg Airport to be a major improvement over earlier models, in particular since the image displayed shows only a generic outline rather than data subjects' actual body contours. However, I see a need for further improvement, and I have asked the Federal Ministry to have the body scanners certified by independent experts on the basis of the common criteria. I also expect the Federal Government to advocate at European level the requirements it has agreed to meet as Europe-wide minimum standards. In addition, the results so far indicate that the scanners still have a very high error rate, so they have not yet met the requirement of providing increased security or of being suitable for routine use.

Before testing began at Hamburg Airport, I inspected the devices at the Federal Police research laboratory, and I will carefully monitor the further progress of the body scanner testing. In an upcoming inspection, I will check first of all whether any data are being stored and whether screening staff conduct follow-up searches in a more private area as required and with the necessary sensitivity. One thing will likely be impossible to avoid: When the scanners are adjusted to detect more dangerous items, then they will also detect many things which are not dangerous.

Box for no. 7.3.1

Resolution of the 79th Conference of Data Protection Commissioners of the Federation and the *Länder* of 17–18 March 2010

Full-body scanners: Many open questions

The attempted Detroit bombing on 25 December 2009 set off renewed debate over the use of full-body scanners in screening airline passengers. This technology is intended to close gaps in security. However, it is still largely unclear what these devices can achieve technically and how they can be integrated into a consistent overall system of aviation security. A decision by lawmakers on whether to deploy such scanners should fulfil at least the following conditions:

1. It is necessary to clarify whether these devices will provide a significant improvement in security. The technical performance and efficiency of this technology are currently subject to serious doubts, especially with regard to their ability to detect low-density materials, such as powdered materials like those used in the attempted Detroit bombing.
2. It is necessary to ensure that the data of screened subjects are not saved after screening is completed. Technical measures should be taken to ensure that body contours are not displayed and that screening images are not saved after screening.
3. Even when these conditions are fulfilled, the use of scanners must not violate the basic rights of persons screened, in particular the constitutional right to human dignity and the right to life and physical integrity. For example, sexual characteristics, prostheses and medical aids (such as colostomy bags) may not be displayed. Harmful impacts on health must be ruled out.
4. Practical tests must be used to demonstrate that these conditions have been fulfilled.

7.3.2 Biometric border checks at airports: Sorting airline passengers into risk categories?

The International Air Transport Association (IATA) has proposed a fundamental overhaul of the system of security checks at airports based on sorting airline passengers according to risk categories.

First, passengers would be identified using biometric features and checked against their booking information. In the next step, passengers would be divided into three categories: known passengers, ordinary passengers and potential threats. Depending on the result of the risk assessment, passengers would be directed to three different “tunnels”, where they would undergo different levels of security checks. While “known travellers” – largely frequent business travellers – would have to undergo a more superficial physical inspection, it seems likely that the other

categories would be subject to more intensive checks, with “potential threats” facing the most intensive searches and questioning.

In my view, however, such categorization is unacceptable.
Passengers would be categorized according to completely opaque criteria. This arrangement would be likely to benefit only business travellers. As a rule, ordinary passengers would see no improvement over the status quo, while those unfortunate enough to be categorized as “potential threats” would be subject to even more extensive, time-consuming and thorough checks. Since all passengers other than “known travellers” would not be aware of their category ahead of time, they would have to arrive at the airport even earlier than they do now to allow time for the extra screening should they be categorized as a “potential threat”. Further, I am critical of the associated comprehensive check of all travellers’ data because data collected for completely different purposes would be used to create a risk assessment, and because other official data and additional behaviour detection techniques during individual interviews would be used for risk assessment. This data check would be combined with a system of individual investigation. In my view, such a system would be extremely discriminatory, so I consider the IATA proposal to be very questionable. If implemented, it would represent further tightening of security at the expense of privacy rights.

The Federal Police screening procedures Automated and Biometrics-Support Border Controls (ABG) (see 20th Annual Report, no. 5.3.5, and 21st Annual Report, no. 4.5.2) and EasyPASS (see no. 3.5 above and 22nd Annual Report, no. 6.4) should also be viewed from this perspective, as they are intended to identify airline passengers with the help of biometric data and would thus constitute a building block in the IATA’s proposed security screening system.

7.3.3 Federal Police introduce electronic criminal records

The Federal Police are currently transferring their criminal records to an electronic system. This is also associated with data protection risks.

During the reporting period, the Federal Police informed me of their decision to replace their conventional paper-based criminal records system almost entirely with an electronic system (eKA).

This change in the keeping of criminal records raises fundamental questions of data protection: Depending on the design, this switch may result in particular in more data

being stored, in duplication of records and in an inappropriate increase in access to data and possibilities for searching records. For example, the Federal Police plan to include a broad range of measures – from law enforcement and threat prevention to other Federal Police tasks assigned by law – thereby expanding the group of persons covered by the electronic records system. Further, all Federal Police offices are to have access to the entire eKA database. The Federal Police databases @rtus (see 21st Annual Report, no. 5.3.1) and Bundespolizeiaktennachweis (Federal Police records system) (see 20th Annual Report, no. 5.3.2) partly overlap the eKA database in terms of function and purpose, which may lead to multiple records of personal data. In designing the electronic criminal records database, it is therefore necessary to consider whether other existing databases will no longer be needed and could therefore be deleted, and how to prevent misuse when so many more Federal Police officers will require only a mouseclick and some additional information to gain access to almost all the data contained in the electronic criminal records. The eKA database also raises familiar questions, such as how to limit the number of records on persons to the smallest necessary and when further storage of records should be reviewed. The Federal Police view the option to enter information about data subject's personality in the electronic criminal records as a special plus.

After a preliminary meeting, I conducted an inspection and advisory visit to the Federal Police Regional Office at Frankfurt Airport during the pilot phase introducing the electronic criminal records system. When this report went to press, the analysis of the large quantity of materials had not yet been completed. I will address this issue in my next annual report and give the results of the review.

7.4 Preventive telecommunications surveillance and telecommunications interception at the source

The Customs Criminological Office is authorized to conduct preventive telecommunications surveillance. It also intercepts telecommunications at the source, i.e. penetrates computer systems in order to listen in on encrypted conversations.

Near the end of the reporting period, I conducted an advisory and inspection visit of the Customs Criminological Office (ZKA) to see how the ZKA uses preventive telecommunications surveillance, i.e. surveillance of e-mails and telephone conversations applied for before criminal proceedings have been initiated against the person under surveillance. The authorization for this serious encroachment on basic rights at an early stage was added to the Customs Investigation Service Act (ZFdG) years ago to give Customs investigators another tool to prevent illegal exports and

imminent violations of the War Weapons Control Act (KWKG) (see 21st Annual Report, no. 5.4.1).

During this visit, it was obvious that the courts have a great influence on the practice of gathering and processing telecommunications data obtained through preventive surveillance. This applies not only to the court order almost always required to conduct such surveillance, but also to the storage of the data obtained. For example, the legal requirement to notify the subject of surveillance is largely determined by court rulings, since court approval is required to postpone or waive such notification. For this reason, I focused my inspection on how the ZKA manages content concerning what is known as the core area of the private sphere.

In addition, I read in a newspaper report that the ZKA had already used telecommunications interception at the source in several cases. This term refers to surveillance of conversations transmitted in encrypted form. The most familiar example is Internet telephony. In order to listen in on such conversations, it is necessary to install software on one of the computers involved which allows access to the data before they are encrypted. In this way, the measure is similar to remote searching of computer hard drives, but unlike remote searching, interception at the source must ensure that access is limited to telecommunications data generated during a conversation; no other data stored on the computer may be collected. The legal basis for telecommunications interception at the source is a very contentious issue. In my view, this measure cannot be based on the same legal provisions as conventional telecommunications surveillance, such as Section 100a of the Code of Criminal Procedure or even Section 23a of the Customs Investigation Service Act. Following the Federal Constitutional Court decision of 27 February 2008 on remote searching of computer hard drives (1 BvR 370/07; see 22nd Annual Report, no. 4.1.1), I believe special legal authorization is required, as was created in Section 20l of the BKA Act.

When this report went to press, I had not yet completed my final review of the information gained during the visit. In particular, apart from the legal monitoring of preventive telecommunications surveillance it is necessary from the technical point of view to understand how the ZKA installs the software needed to intercept at the source and check that it collects only data generated during the ongoing telecommunications connection. I will report on the results in the next Annual Report.

7.5.1 Should the federal and *Länder* domestic intelligence agencies be allowed to set up a comprehensive information pool?

Expanding the intelligence database of the federal and Länder authorities for the protection of the constitution (NADIS) into a comprehensive knowledge network (NADIS-WN) violates legal restrictions and is therefore unlawful.

The federal and *Länder* authorities for the protection of the constitution are required to store identifying information called basic data (e.g. name, address, etc.) as well as the file reference for persons and organizations under surveillance in a separate index file (NADIS). In this way, each authority for the protection of the constitution can find out whether the others have information on a person or organization. But NADIS does not show what information this is. Text excerpts or text files, such as surveillance reports, may be stored in NADIS only in strictly regulated exceptions.

Now NADIS is to be expanded into a comprehensive knowledge network (NADIS-WN). This means a change of paradigm to an information pool in which every network partner stores as many data as possible on NADIS-relevant persons and organizations. Other network partners will be able to read and automatically analyse this information (for example using full-text search). The first project phase (NADIS-WN 1.0) is already under way and is to go into nation-wide operation on 4 October 2011. A major goal of this phase is storing unstructured source documents and information, such as source reports, reports from other intelligence services, surveillance reports, newspaper reports and publications (e.g. Internet content).

The problem is that such documents may also contain information on persons who do not come under the jurisdiction of the Federal Office for the Protection of the Constitution (BfV) and which up to now may not be kept on file. This includes information on persons under age 16 and non-suspicious persons who have come into contact with the target at random or unawares, such as family members, neighbours, co-workers, supervisors or journalists who contact or report on such persons or organizations for professional purposes. Under current law, the BfV may store their data in paper-based files but not in databases and may not analyse them for intelligence purposes under any circumstances. NADIS-WN 1.0 would cross this legal boundary (like DOMUS; see 18th Annual Report, no. 14.1 and 20th Annual Report, no. 5.5.2).
The law deliberately distinguishes between storing data in paper and electronic files. The law was intended to keep these data out of electronic files where they could be filtered, analysed and sent around the world in less than a second thanks to electronic technology. The Federal Constitutional Court too has always stressed that

merely by transferring personal data from paper files to electronic files constitutes an intrusion on the basic right to determine the use of one's own data. According to the court, data stored in electronic files, unlike those in paper files, can be accessed at any time regardless of their location within seconds. In the court's view, the quantity of data available for electronic processing creates a special potential for intrusion which would not exist in the case of paper files, which would have to be processed conventionally.

The Federal Ministry of the Interior believes that storing such data in NADIS-WN does not represent unlawful intrusion, because technical safeguards prevent the data from being analysed separately. However, this contradicts the law and the Federal Constitutional Court as referred to above. Further, technical safeguards can be suspended relatively easily and quickly, as pointed out in a resolution by the Conference of Data Protection Commissioners of the Federation and the *Länder* at their 80th session on 3-4 November 2010 (see box for no. 7.5.1).

Saving source documents and information in NADIS-WN 1.0 would also have serious consequences: If a non-suspicious person later becomes suspicious and her information is lawfully stored in NADIS-WN 1.0, a comprehensive search would turn up also those data stored unlawfully when she was still a non-suspicious person.

To sum up: NADIS-WN 1.0 does not comply with existing law. Implementation measures which have already been taken must therefore be reversed without delay. I have informed the Federal Ministry of the Interior. No comments were available by the time this report went to press.

Box for no. 7.5.1

Resolution of the 80th Conference of Data Protection Commissioners of the Federation and the *Länder* of 3/4 November 2010

No full-text searching in databases of the security authorities

The Conference of Data Protection Commissioners of the Federation and the *Länder* calls on the Federal Government and the *Länder* governments to design full-text based databases in compliance with the very restrictive constitutional boundaries.

The federal and *Länder* security authorities (domestic intelligence, police) are currently expanding their electronic filing systems. In doing so, they are including

data which up to now have been available only in paper form and are pursuing comprehensive full-text processing and search options which will make it possible to search for any word or other text in a document.

This has serious consequences. The files also include information on persons other than those targeted by the official measures. The new system will make it possible to conduct targeted electronic searches of information on innocent persons who unknowingly came into contact with the target person and who happen to be mentioned in the file.

This change of paradigm contradicts existing law, which states that security authorities may save and transmit selected personal data in electronic files only under strict conditions. Today, the types of data and data fields to be stored must be defined in detail in specific orders on opening and maintaining files. The data protection commissioners must be consulted in advance.

The ability to conduct full-text searches would override these data protection safeguards. It would no longer be possible to enforce the restrictions on data processing. The legal boundaries are anchored in the constitution. The law deliberately sets stricter requirements for personal data stored in electronic filing systems, because, as the Federal Constitutional Court emphasizes in its established rulings, electronically stored data can be accessed and comprehensively analysed within seconds, regardless of their location. According to the court, this represents a serious intrusion on data subjects' basic right to control the use of their data, especially when the data were gathered and processed without the data subject's knowledge.

These constitutional safeguards to protect data subjects’ right to control their own data, in particular the separation of informational powers, would cease to function if all information were to be subject to unlimited electronic full-text searching.

There would be no difference in legal terms if technical mechanisms (temporarily) hindered such analysis, because such mechanisms can be altered technically at any time, and because temporary barriers to the possibility of searching would prevent neither intrusion on the right of data subjects to control their own data nor the violation of the restrictions on preventive data processing set by the Federal Constitutional Court.

If these data protection risks exist within general administrative agencies, they are even greater in security authorities. This applies especially to the intelligence services, which are allowed to gather information on legal behaviour and intelligence, the relevance of which has not yet been established. Such system-wide, targeted searching could have serious consequences for possibly innocent data subjects. These risks must be taken into account and dealt with already in the planning phase when expanding IT systems.

7.5.2 Problems with the right to information from the domestic intelligence agencies

When the Federal Office for the Protection of the Constitution (BfV) refuses requests for information, the grounds for refusal are supposed to be documented. The BfV is also responsible for information received from the Länder offices for the protection of the constitution (LfV).

The right to information covered by Section 15 of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (Act on the Protection of the Constitution, BVerfSchG) is essential to exercising the basic right to determine the use of one's data. Already in my 22nd Annual Report (no. 4.7.1) I called on the BfV to comply with the constitution when responding to requests for information. Now there is again cause for criticism.
In accordance with Section 15 (1) of the above-mentioned Act, the BfV must furnish data subjects free of charge with information on the data it has stored relating to them, if they refer to concrete matters and prove to have a special interest in the information they have asked for. The BfV has sometimes set its standards too high with regard to these conditions.
And in cases when it is allowed by law to deny a request for information, it has not reviewed the individual request or documented it appropriately but has refused the request out of hand.

According to Federal Constitutional Court rulings, this is not allowed. In its decision of 10 October 2000 (1 BvR 586/90), the court stated that the reasons for refusing a request for information are to be recorded so they are available for review by third parties. The court also said that the reasons for refusal must be clear and understandable. After meeting with the BfV, I was able to ensure that these requirements of the court have now been implemented by all the relevant departments. As a result, I can now review the reasons for refusal at least in terms of

their plausibility. However, this does not completely solve the problem. If the only information the BfV has on a data subject is information received from an LfV, then the BfV cannot, as a rule, review the individual request: In their own interest, the LfV often fail to provide the (background) information necessary to determine for example whether providing the information would endanger an LfV source. In these cases, the LfV tell the BfV only that providing information would endanger the source. But this is not enough for the BfV to refuse an information request. When the BfV accepts information from an LfV, this information becomes the legal property of the BfV, meaning that the BfV must meet all the legal requirements concerning this information. It cannot delegate its responsibility to the LfV, i.e., it is not sufficient for an LfV to carry out a review relevant for an information request submitted to the BfV. The BfV itself must review the individual request. To do so, it requires the necessary information from the LfV.
It is unacceptable under both constitutional and data protection law that many LfV massively resist this requirement and that data subjects must resort to legal proceedings to enforce their right to information. The BfV concedes that it will lose in court due to the LfV's improper conduct. I call on the federal and *Länder* governments to enable the BfV to provide information in compliance with the law. This means that the LfV must inform the BfV of their reasons for denying information requests and must report the review of the requests in a way that upholds the interest of the LfV in maintaining confidentiality.

7.6 Intelligence services

7.6.1 Data processing conducted by the Federal Intelligence Service

In inspecting a large-scale central database of the Federal Intelligence Service (BND) containing several million files, I found violations of data protection law. Until a system which complies with data protection law is created, these files are to be used operationally only in exceptional cases.

Most of the violations are due to structural shortcomings in the database. Among other things, the BND has failed to carry out any resubmission checks or reviews to assess whether data items qualify for erasure as stipulated in Section 5 (1) of the Act on the Federal Intelligence Service in conjunction with Section 12 of the Act on the Protection of the Constitution. As a result, the database contains a large quantity of data, both public and covertly obtained, which should have been reviewed and in some cases deleted long ago. Further, old data kept by the BND even before the present database, which has existed for many years, was created were transferred to

the database without being reviewed first. Some of these data are as old as the BND itself.

In view of the vast daily influx of data, this database is tantamount to a constantly growing reservoir of information with no outlet.

Following in-depth discussion of this problem area, I called on the BND and the Federal Chancellery as the competent supervisory authority to ensure that this database is handled in compliance with the law. In the BND's view, this database represents its "backbone", an indispensible data collection which cannot be taken apart and subjected to a comprehensive revision in accordance with the prevailing statutory requirements on account of the vast volume of data it contains and the attendant technical difficulties. The BND concedes that this might be possible in conjunction with the BND’s relocation to Berlin. In order to alleviate my concerns in the short term, the Federal Chancellery proposed moving all data stored for more than ten years out of the current online database and into a separate archive, to be used only in special cases for current operational purposes, such as the fight against terrorism or proliferation.

I am open to this proposal, particularly since the Federal Chancellery has said that the archive would be kept only temporarily, until the database is restructured in compliance with the law. I am to be informed in advance of the further plans.

8.1.1 The 2011 census

The 2011 census has begun. For the first time since 1987 (in the former West Germany) or 1981 (in the former East Germany), Germany is conducting a population census to implement Regulation (EC) No 763/2008. This census will be primarily register-based.

Every registration authority in Germany submitted its data files to the statistical offices by the deadline on 1 November 2010. Additional data are to be submitted on 9 May and 9 August 2011. A housing census, a sample survey of households and surveys of communal housing (e.g. nursing homes, dormitories, emergency housing) will also be conducted on 9 May 2011.

The Act on the Register-Based Census in 2011 (Zensusgesetz 2011, ZensG 2011), which entered into force on 16 July 2009, provides the legal basis for the population census. I already reported on the draft legislation (see 22nd Annual Report, no. 5.5).

Unfortunately, my recommendation not to collect personal data on sensitive types of communal housing (such as prisons, where the information could result in social discrimination against the persons concerned) was not followed.

And further topics were added to the household survey while the Act was being passed. The topics “Legal membership of a religious community under public law” and “Religious affiliation, faith or world view” are not provided for in European law. During the legislative process, I repeatedly questioned the need for and appropriateness of these topics. Unfortunately, my objections were ignored and these topics were included in the Act on the Register-Based Census in 2011. However, answering the question regarding religious affiliation will be voluntary.

For the housing survey, all homeowners will be asked to complete a written survey on their property, including questions on the year the home was built, the type of heating, the size of the home and how it is used (Section 6 (2) of the Act).

For the household sample survey, 9.6% of the population will be asked to respond. Questions cover personal information and information about education, training and occupation (Section 7 (4) of the Act). For the survey of communal housing, residents will be asked to provide their month and year of birth, family status and date on which they entered communal housing. Although, contrary to my recommendation, the law allows personal data to be collected on residents of sensitive communal housing, the Federal Statistical Office has at least developed a special procedure for processing these data to do justice to these residents’ special need for protection.

Other persons in need of special protection are those whose registration data are not to be disclosed due to danger to their life or well-being, for example persons participating in a witness protection programme. In order to ensure that such persons receive the necessary special protection, I recommended excluding their addresses entirely from the household sample survey.

The statistical offices developed a generic security strategy for the 2011 census, which I was allowed to review. In terms of methodology, the strategy is oriented on the standards issued by the Federal Office for Information Security (BSI). Section 13 of the Act states that each person is to be issued an identification number. I found it especially important that this number should not reveal the person to whom it is assigned, so I persuaded the Federal Statistical Office to encrypt the personal identification number using a hash function.

In addition to the identification number referred to in Section 13 of the Act, additional numbers will be assigned as internal statistics for organizational purposes only. One of these numbers is the respondent ID within the housing census. This number identifies specific persons for internal statistics and to compile their data for the housing census. The respondent ID consists of a series of numerals which in themselves reveal no information. However, as an internal identifier, the respondent ID may not be used outside the statistical offices, as I was able to convince the Federal Statistical Office. The original plan called for using the respondent ID as the number on the questionnaire forms in the housing census. Instead, now every questionnaire is assigned a non-systematic number which can be linked within the official statistical offices with the respondent ID using an algorithm.

I will be intensively monitoring the practical implementation of the 2011 census in close cooperation with the data protection commissioners of the *Länder*, who are responsible for the state statistical offices, the cities and municipalities. In particular, I will be checking compliance with

- legal restrictions on data use,
- data deletion at the earliest possible date, and
- a high standard of data security.

8.2 Law on foreigners

8.2.1 Central Register of Foreigners: Time to provide better protection for the data of EU citizens!

The Central Register of Foreigners does not sufficiently implement European law on when data of EU citizens may be stored. Now lawmakers must take action.

The Central Register of Foreigners (Ausländerzentralregister, AZR) contains personal data on all foreigners residing in Germany longer than three months, including EU citizens. With its decision of 16 December 2008 (C-24/06), the European Court of Justice found that this storage of data on EU citizens in a central register such as the AZR and the transmission of these data to other agencies was permitted only under strict conditions (see 22nd Annual Report, no. 16.1). Following this decision, I decided to check the AZR for compliance with data protection law. I found that the European Court of Justice requirements have not been implemented

with regard to automated retrieval, which applies to most of the data retrieved. Nor had notices on EU citizens been deleted, so data stored in the AZR on EU citizens could still be transmitted, for example to security authorities for law enforcement purposes, even though the European Court of Justice had explicitly stated that this was not permitted. I complained about this violation of European law pursuant to Section 25 (1) no. 1 of the Federal Data Protection Act. Nor had the agency responsible for the AZR taken any technical or organizational measures to ensure that data could be retrieved only for the purposes recognized by the European Court of Justice and only by the authorities with responsibility for law on foreigners.

In response, the Federal Ministry of the Interior promised to delete any remaining notices on EU citizens. The technical measures to implement the rules on automated retrieval are to be taken as soon as the process of amending the Act on the Central Register of Foreigners (AZR Act, AZRG), which is currently under way, has been completed. However, the draft bill initially presented by the Federal Ministry of the Interior for approval by the other federal ministries did not sufficiently transpose the European Court of Justice requirements into national law. For this reason, I have advocated significantly reducing the amount of data stored in the AZR on EU citizens and allowing these data to be transmitted only for residence law purposes and only to the authorities responsible for this area.

The legislative process had not yet been completed at the time this report went to press. I will continue to monitor the process and work for rapid technical implementation in the AZR as soon as the Act has been amended.

The research clause agreed among the ministries with my participation in 2007 is to be included in the amended Act, which I view positively (see 21st Annual Report, no. 7.1.3). This clause will make it possible to use the AZR data on third-country nationals for research purposes.

8.2.2 The electronic residence title: A document in credit-card format, with fingerprints

With the introduction of the electronic residence title, foreigners authorities will require not only photographs but also fingerprints of foreigners living in Germany.

In implementing Regulation (EC) 380/2008, the Federal Ministry of the Interior created the legal basis for introducing electronic residence titles for foreigners who are not EU citizens. Starting in September 2011, the new electronic residence titles

are to be issued in credit-card format, like the new national identity card (see no. 3.2). The residence card will contain a chip on which two fingerprints and a digital photo of the cardholder are stored as biometric identifiers, which is required by the European regulation (cf. box for no. 8.2.2). Unlike the identity card, for the residence card two fingerprints are mandatory.

The new residence card will offer the additional option of serving as an electronic proof of identity for legal transactions on the Internet.

As part of my participation in the legislative process, I worked to ensure a high level of data protection and security for the biometric identifiers stored on the chip and for the electronic proof of identity function. The same data protection requirements as for passports (with regard to biometric features see 22nd Annual Report, no. 6.3.1) and the new identity card (with regard to the proof of identity function, see no. 3.2 and 22nd Annual Report, no. 3.3) are to be applied accordingly to the residence card. I will carefully monitor to check whether these data protection requirements are carried out, especially with regard to protected access to the biometric data stored on the chip.

I also oppose calls to store the biometric identifiers in central registers, such as the Central Register of Foreigners.

Box for no. 8.2.2

Electronic residence title for foreigners

9 Financial matters

9.1 CD-ROMs of data on tax cheats: Data protection should not go out the window because of government budget deficits!

The debate over buying CD-ROMs of tax data from questionable sources has revealed tension between the possibilities and limits of government action under the rule of law. I believe special legislation is needed to reconcile the conflicting and protected interests.

The debate over whether the government should buy from “shady sources” a CD-ROM containing data files on suspected tax cheats caused controversy among data protection officials and the general public. A data dealer who had illegally acquired data files on customers of a Swiss bank offered to sell this information to the German government. Those in favour of buying could not understand why the German tax authorities should not use these data due to data protection concerns about their source, arguing that such data should not be protected, as doing so would cover up tax evasion. For this reason, they argue, the German tax authorities are not prevented from working with informants.

Nonetheless, I spoke out against buying data files from illegal sources. A government based on the rule of law must act within the law. The relevant requirements for official investigations are defined in particular by the Code of Criminal Procedure, which does not allow covert access to information technology systems. Nor do the provisions of the German Fiscal Code applicable to tax investigators allow covert searches of third-party computers and data stored there to seek evidence of tax evasion. The informant apparently acquired the data he was offering by these or

similarly illegal means. Data acquired in violation of data protection regulations remain unlawful even if they are to be used for a legitimate purpose. A government based on the rule of law may not evade its legal limits by relying on unlawful actions by third parties.

The possible consequences of rewarding “data thieves” constitute a special problem: If the government pays informants for CD-ROMs with illegally acquired data files, instead of calling them to account for their criminal activity (and possibly extraditing them), one must ask whether the government is indirectly encouraging the theft of confidential personal data.

Buying a CD-ROM of tax data from an illegal source represents a special investigative measure which in my view is permissible only on the basis of special authorization not granted by current law. Authorities in a state based on the rule of law must conduct their investigations in a clear and transparent way. This includes transparency with regard to how information makes its way to the tax authorities.

For this reason, I have called for concrete federal regulations to deal with offers of data files on tax evaders. Lawmakers are called on to reconcile the conflicting interests in such cases. In any case, buying such data files should only be a last resort. The tax authorities must have already exhausted the information-gathering means at their disposal, including information-sharing with foreign tax authorities and the possibility of mutual legal assistance (see no. 9.7). And any regulations must not encourage the business model of illegal data acquisition or illegal data trafficking. Apart from this specific issue, I also believe that the question of dealing with data from “shady sources” will assume increasing importance for the law enforcement authorities due to technological progress. This is another reason for creating special regulations.

In connection with thoughts on a legal basis, I believe it is also necessary to discuss the use of purchased information further. In the meantime, the Federal Constitutional Court has ruled that the initial suspicion required to search a home may be based on data from a CD-ROM sold to the Federal Intelligence Service by an informant from Liechtenstein (Federal Constitutional Court, decision of 9 November 2010, 2 BvR 2101/09). However, this ruling does not conclusively clarify the question of whether acquiring such data is permitted.

9.2 The power of tax identification numbers

The government keeps a central record of all German citizens using tax identification numbers. Expanding the stock of data or linking different data pools which are based on the tax ID number entail serious risks to the right to determine the use of one's personal information.

Ever since the tax identification number was introduced, I have pointed to the danger that it could turn into a personal ID number linked to other databases, enabling the creation of comprehensive personal profiles (see 22nd Annual Report, no. 9.1). The danger is less that the tax ID number becomes a general identifier than that its use is gradually expanded to other applications, which would ultimately have the same effect.

Unfortunately, recent developments tend to confirm my fears: The Annual Tax Act of 2010 assigned new functions to the tax ID number, which lawmakers intended to better enforce the tax laws and improve the distribution of the tax burden. However, the new law also gives the government new possibilities to store a wide variety of data in a central database on individuals identified by their tax ID number. The main problem is that the tax ID number is increasingly being gathered and processed by private-sector bodies,

for example under the rules introduced in the Citizens Relief Act (Bürgerentlastungsgesetz Krankenversicherung) pursuant to Section 10 (2) and (2a) of the Income Tax Act (EStG). These rules allow private health insurance companies to collect and process tax ID numbers so that insured persons may claim relevant expenses when filing their tax statements. As numerous letters to my office indicate, the persons affected fear becoming "transparent taxpayers". In particular, they criticize the fact that they can claim the full extent of preventive medical expenses only if they agree to have their health insurance company collect and process their tax ID number.

However, effective consent under Section 4a (1) first sentence of the Federal Data Protection Act depends on the free decision of the data subject, which in turn requires a real possibility of choice, which does not exist in this case. I have therefore recommended to the Federal Ministry of Finance that it provide taxpayers with alternative ways to provide proof of their preventive medical expenses, for example by providing the relevant receipts to the tax office. Unfortunately, the ministry has so far failed to follow my recommendation.

Another problem is that, due to the variety of bodies using the tax ID number for all sorts of purposes, data subjects cannot find out without extra effort which of these bodies are storing which of their data. The result would be a "creeping" accumulation of their data without the data subjects' knowledge. I am also critical of the fact that new legislation may be introduced to allow further tax-relevant data to be stored under the tax ID number, as has already happened in the case of income-tax-relevant data under Section 39e of the Income Tax Act (see no. 9.3). Because tax law extends into almost all areas of life, very extensive data files could result. These data pools might also allow conclusions to be drawn about facts with no direct relation to taxes.

The Finance Court in Cologne, which in a test case examined the lawfulness of tax ID numbers collected on the basis of Sections 139a and 139b of the German Fiscal Code, shares my concerns (Finance Court Cologne, decision of 7 July 2010, 2 K 3093/08). Although the court expressed "significant doubts" concerning the constitutionality of the tax ID number, these doubts were not sufficient to convince the court of a constitutional violation, so the matter was not referred to the Federal Constitutional Court.

Given the sensitivity of these data and the possible threat arising from automated data processing in connection with the tax ID number, I already pointed out at an early stage the need to secure the database with a comprehensive IT security strategy specifically tailored to the processes in use. The Federal Ministry of Finance let me see this strategy only after I made a formal complaint under Section 25 (1) of the Federal Data Protection Act. I am currently examining the numerous documents and plan to monitor the handling of tax data during an advisory and inspection visit to the responsible Federal Central Tax Office.

9.3 Introducing the electronic wage tax card

Paper-based wage tax cards are to be replaced by an electronic process effective 1 January 2012, bringing automation in the tax administration to a new level, both qualitatively and quantitatively. This project raises many data protection questions.

The database of tax identification (ID) numbers at the Federal Central Tax Office (BZSt) is currently being expanded to include data needed for wage tax withholding. The electronic wage tax withholding information (German acronym ELStAM) kept in the database in accordance with Section 39e of the Income Tax Act covers not only tax-relevant data, but also some sensitive personal data, such as religious affiliation,

family status and information about family members (see box a for no. 9.3). Although the introduction of the electronic wage tax card will not result in any new personal data being collected, data previously kept by different register and tax authorities will now be compiled into one central database for the first time. The expanded database will contain sensitive tax data for more than 40 million employed persons when it goes into operation. I have already pointed out the associated risks repeatedly (see 22nd Annual Report, no. 9.3).

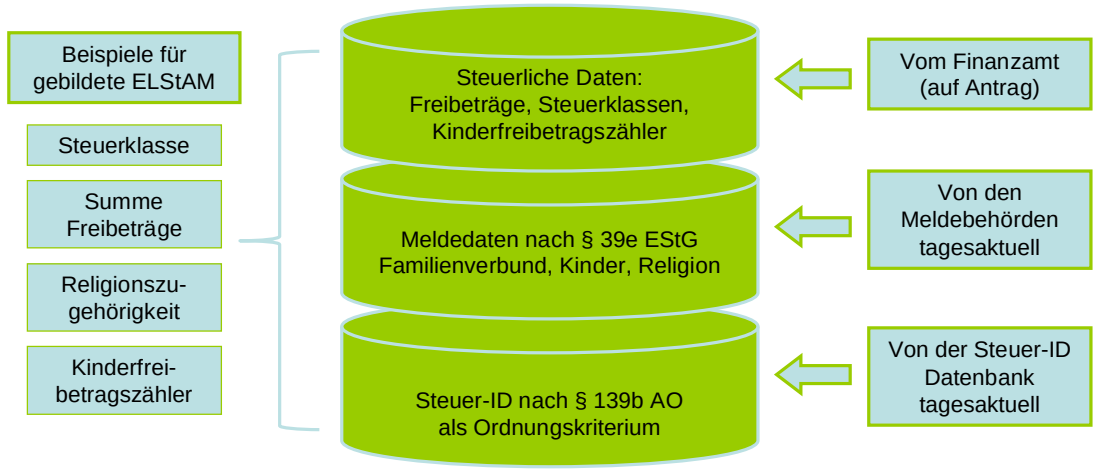
With the Annual Tax Act of 2010, supplementary provisions on the electronic wage tax card were adopted in Section 52b of the Income Tax Act. During the legislative process, I advocated improving the planned data protection requirements. I welcome the fact that the German Bundestag followed my recommendation to have the tax offices inform affected taxpayers about the expanded information in the database well in advance of the new procedure (see Bundestag printed document 17/3549, p. 29 and 17/3349, p. 44). The Federal Government's original draft bill did not provide for such an arrangement. This will give affected taxpayers the chance to check their data held by the BZSt for accuracy and correct them before their employers retrieve these data.

The stored data files are to be accessible to about 4 million employers nation-wide. To access these data, employers must be authenticated via the ELSTER-Online website. I view this process with some scepticism, as the ELSTER website primarily serves to transmit taxpayer documents to the tax administration electronically (see no. 3.6). There are doubts as to whether the website is an appropriate channel of access for employers, because the current technical framework conditions do not ensure adequate proof of employers' identity and authorization to access the data. Due to the sensitive nature of the data files, the risk of unauthorized access must be ruled out as far as possible. The tax administration must take the necessary technical and organizational measures to do so. With this in mind, I welcome the new Section 52b (8) of the Income Tax Act allowing employed persons to block all access to their data via the responsible tax office or to select employers who may access their data or not.

With regard to the transfer of tax-relevant data from local register authorities to the BZSt in order to build up the ELStAM database, I have explained that it is necessary to develop a security plan tailored to the specific IT application in parallel with the data transfer. The Federal Ministry of the Finance has agreed to develop such a security plan, which I will examine once it is completed and has been sent to me. Together with the data protection commissioners of the *Länder*, I will continue to work

on behalf of better protection for the sensitive wage tax data stored in the central tax database (see also the Resolution of the Data Protection Commissioners of the Federation and the *Länder* of 24 June 2010, box b for no. 9.3).

Kasten a zu Nr. 9.3
Inhalt der ELStAM Datenbank



Box b for no. 9.3

Resolution of the Conference of Data Protection Commissioners of the Federation and the *Länder* on the expansion of the central tax database to include electronic wage tax withholding information of 24 June 2010

Expanding the tax database entails major risks

The Bundesrat and Bundestag will soon be discussing the planned provisions in the Annual Tax Act of 2010 on expanding the central tax database. Electronic wage tax withholding information (ELStAM), such as sensitive information on religious affiliation and family members, is to be added to the database. The data protection commissioners of the Federation and the Länder find it necessary to examine these provisions in a critical light to determine whether they suffice for data protection

purposes and adequately uphold the rights of the employees concerned. The following points require special attention:

– *Informing employees in advance*
  The paper-based wage tax card is to be replaced by the electronic wage tax card. In order to ensure that the transition to the new process is transparent, affected employees must be informed of the specific information about them before the new system goes into operation. This will enable them to correct any errors in the data at the Federal Central Tax Office before they are accessed by the employer.

– *No preventive data retention*
  The central database is supposed to keep data files also on those persons who are not in employment which is subject to the wage tax. The retention of data files for possible future use is highly questionable under constitutional law. Data files should be kept only on those persons who are required to pay the wage tax.

– *Preventing unauthorized retrieval of data*
  About 4 million employers nation-wide will have access to the stored data. Retrieval of the electronic wage tax withholding information should be possible only after employers or third parties commissioned by them have verified their identity and provided their tax number. The procedure must ensure that only authorized employers can retrieve data files. Whether this will be achieved has yet to be clarified. If unauthorized data retrieval cannot be ruled out, then access should be possible only with the participation of the employee concerned.

– *The system should not be launched without a security plan tailored to the specific IT application*
  The expanded central database will contain highly sensitive tax data on more than 40 million employees. A high standard of data security must be in place by the time the system goes into operation. This requires a comprehensive and complete application-specific IT security plan. Experience shows that developing IT security plans for databases on this scale takes a significant amount of time. The IT security plan must be completed before the work of expanding the database begins.

9.7 Sharing tax-related information with other countries

International sharing of tax information has recently assumed greater importance. Data protection law must be respected here as well.

As a result of the global financial and economic crisis, international cooperation on tax matters is to be increased, especially with regard to information-sharing among tax authorities. Under the supervision of the Organization for Economic Cooperation and Development (OECD), detailed standards for such information-sharing have been developed. Germany is currently making bilateral agreements with countries which have important financial centres; these agreements are intended to enable information-sharing in compliance with the OECD standards.

In the framework of my participation, I work to ensure that the procedures for intergovernmental sharing of tax data pay attention to data protection concerns. This applies above all to automated information-sharing, in which personal data are transferred periodically in the absence of a specific request; and to spontaneous information-sharing, in which one country transmits information which may be relevant for other countries without being asked. These two forms of information-sharing represent a much more serious infringement of the right to determine the use of one's data than convention data transmission in response to a request and therefore must be precisely defined as to purpose and extent.

10 Business and transport

10.1 Binding corporate rules

The procedure for adopting binding corporate rules (BCR) for transferring data from the EU to third countries has been significantly speeded up. During the reporting period, I was able to successfully complete the review of the BCR of Deutsche Post AG using this procedure.

Under the EU Data Protection Directive, personal data may be transferred to third countries which do not ensure an adequate level of data protection on certain conditions (Article 26, Directive 95/46/EC). To do so, companies must make adequate data protection guarantees, among other things using binding corporate rules (BCR). During the reporting period, the Art. 29 Data Protection Working Party continued its efforts to simplify and standardize the BCR procedure. The procedure for reciprocal recognition agreed in 2008 between the data protection supervisory authorities of several Member States significantly expedited the process. With this

procedure, if the supervisory authority gives the BCR of a company in the lead Member State a positive review, this is sufficient grounds for the authorities in the other Member States to approve the BCR as well (see 22nd Annual Report, no. 13.2.3). Nineteen data protection supervisory authorities are currently participating in the procedure. In addition, the catalogue of frequently asked questions to inform companies what European data protection supervisory authorities require of BCR has been revised (WP 155 Rev. 4 of 8 April 2009).

In 2007, Deutsche Post AG, a globally active group of companies which constantly shares customer and employee data across international borders, asked me to oversee the European procedure for reviewing binding corporate rules in accordance with the requirements of the Article 29 Working Party. Because the procedure for reciprocal recognition was established during the approval process, Deutsche Post AG's BCR were reviewed using this procedure at European level and the review was completed in December 2010. I also issued the approval to transfer data in accordance with the BCR presented under Section 4c (2) of the Federal Data Protection Act. The majority of European supervisory authorities agrees that this approval needs to be issued only once. When it introduces its BCR, Deutsche Post AG will create a network of data protection commissioners throughout the entire group.

10.8 A Europe-wide motorway toll? Only with good data protection!

Europe is growing together – toll collection is to be simplified in future. It is possible to make phone calls world-wide without switching mobile telephone carriers; the European Commission hopes to introduce similar "roaming" for roadway toll collection too.

For years, I have dealt with data protection aspects of electronic toll collection (in the 19th Annual Report, no. 29.1, for the first time at length). Now the question has come up whether Germany's stricter data protection rules for the HGV toll could be undermined when European law is implemented.

Due to Directive 2004/52/EC of 29 April 2004 on the interoperability of electronic road toll systems and Commission Decision 2009/750/EC of 6 October 2009 on the definition of the European Electronic Toll Service, the Member States are required to create the necessary conditions for introducing a European Electronic Toll Service (EETS). In order to enable electronic collection of all sorts of road use fees on the entire Community road network, the internal market will be opened to European

operators. The declared aim is to produce enough interoperability so that a service operator can provide users with one contract, one on-board device per vehicle and one invoice. The positive effect for users (e.g. large hauliers operating Europe-wide) is supposed to be that in future they will be able to choose their EETS operator themselves, resulting in greater convenience and a reduced administrative burden. EETS is to supplement the national electronic road toll systems in the Member States.

The Federal Ministry of Transport, Building and Urban Development (BMVBS) included me in the implementation of the European requirements at a very early stage. Every Member State was required to provide an Internet-based platform (EETS register) with all information for potential service operators by 9 July 2010. This register was set up at the Federal Office for Goods Transport (BAG). By 9 October 2010, the register was also supposed to contain all legal, technical and organizational requirements for the EETS area, i.e. the road network subject to tolls, as well as information about the national register office. In addition, the register must show the registered EETS operators based in Germany and the contracts concluded between the Federal Office for Goods Transport and the EETS operators. Extensive information is now available to all on the website www.bag.bund.de.
Before setting up the register, the BMVBS asked me for advice on data protection law. My recommendations were incorporated into Document 4.1, *Mauterhebung im EETS-Gebiet ABMG und Mauttransaktionskonzept* (Toll collection in the EETS area Motorway Toll Act for Heavy Goods Vehicles (ABMG) and toll transaction strategy), available on the BAG website. The explicit mention there of the strict restrictions on data use in the ABMG give me hope that these will not be circumvented by opening the internal market. I will continue to monitor this issue and discuss it with my European colleagues as necessary.

12 Protection of employee data

12.1 Protection of employee data: Good things take time?

In summer 2010, the Federal Government presented a draft bill on the protection of employee data intended to replace Section 32 of the Federal Data Protection Act which entered into force in 2009. However, I still see a need for major improvements in key areas.

It seems that spectacular data protection scandals (see no. 12.2 below) are necessary to push the decades-long effort to develop legislation on protecting employee data.

Initial activities were undertaken in 2009 with the aim of anchoring in law data protection rules for employment contracts. On 16 February 2009, a round table invited by the Federal Minister of the Interior focused on the necessary improvements to data protection for workers. Social partners and I were also invited to the round table. Afterwards, the Federal Government agreed to create a basic provision in the Federal Data Protection Act to strengthen the protection of workers' data. This provision was to be drafted by an interministerial working group in which I was to participate.

In parallel, lawmakers responded to the data protection scandals by adopting not only a basic provision on employee data protection as part of the second revision of the Federal Data Protection Act (see no. 2.2) but also rules on comparing employee data with other data for law enforcement purposes (Section 32 BDSG). This was the first legal provision stating that personal data gathered for employment-related purposes could not be used for any other purpose. However, it failed to deal with many other issues concerning the use of personal data before, during and after the end of employment.

Shortly before the 2009 Bundestag elections, the Federal Ministry of Labour and Social Affairs published the draft Act Governing Data Protection in the Employment Sector. After the elections, the SPD parliamentary group introduced this draft bill in the Bundestag without revisions (Bundestag Doc. 17/69). This draft calls for a separate Act Governing Data Protection in the Employment Sector. By contrast, the parties in the governing coalition agreed on 26 October 2009 to incorporate employee data protection into the Federal Data Protection Act.

The coalition agreement of the new Federal Government announced improvements to employee data protection. But the Federal Ministry of the Interior's draft legislation provided in late March 2010 failed to carry out key goals improving workers' constitutional right of privacy. In its Resolution of 22 June 2010 (see box for no. 12.1), the Conference of Data Protection Commissioners of the Federation and the *Länder* therefore expressed serious criticisms.

In the course of the subsequent discussions and in the framework of interministerial coordination, some improvements were made and included in the draft legislation

adopted by the Federal Government on 25 August 2010. For example, the rules on covert investigations, video monitoring and data screening were improved. I view as positive the fact that covert data screening is to be allowed only as a last resort. Covert investigations may be conducted only when there is a suspicion of wrongdoing. Another achievement is that the first step of data screening must be conducted using data which have been depersonalized or rendered anonymous. And covert video monitoring will not be permitted.

Apart from these positive elements, I see a further need for improvement:

- Data screening should be permitted only for a specific reason. In my view, routine data screening to detect suspicious circumstances is unreasonable.
- The underlying rule for covert data processing also provides for the purpose of "preventing further crimes". I cannot imagine a scenario in which this rule would be needed, as such measures are to be directed only against employees who have already been convicted of a crime and would hardly still be at work.
- Also problematic is the plan to allow employee data to be used for a wide range of behavioural and performance monitoring. For example, Section 32i (3) of the draft amendment to the Federal Data Protection Act, which mainly covers e-mail data, contains wording to this effect. I find this too broad.
- The permission to conduct overt video monitoring in the draft amendment is also far too broad and would in fact be worse than the status quo. For example, video monitoring would be permitted for "quality control", however that may be defined.
- There is no clear rule for cases in which both work-related and private use of telecommunications is allowed. Such a provision could also be anchored in the Telecommunications Act, although this would have the disadvantage that the provisions on using e-mail at work would be in two different laws.
- The provision requiring employees to inform their employer of data protection violations before contacting the data protection supervisory authority (Section 32l (4) of the draft amended Federal Protection Act) unreasonably restricts the rights of employees.

The draft legislation is currently under discussion in parliament. I will continue to exert pressure so that the protection of employees' personal data receives the attention appropriate to technical developments and current changes in the world of work (see most recently 22nd Annual Report, no. 11.1).

I continue to hope that, once the legislation on employee data protection is passed during this legislative term, we will be able to say: "Good things take time."

Europe and international affairs

13.1 Treaty of Lisbon brings changes for data protection

The Lisbon Treaty's entry into force represents a milestone for European law on data protection.

The Treaty of Lisbon, which the heads of state and government of the 27 European Union Member States signed on 13 December 2007, entered into force on 1 December 2009 (consolidated version in OJ C 83 of 30 March 2010, p. 47 ff.). The Treaty amended the two founding treaties of the Union: the Treaty on European Union (TEU) and the Treaty establishing the European Community (EC Treaty), now called the Treaty on the Functioning of the European Union (TFEU).

The Lisbon Treaty has made fundamental changes to the system of EU law by ending the pillar structure of the EU policy areas introduced by the Maastricht Treaty. The previous Title VI of the TEU governing police and judicial cooperation in criminal matters ("Third Pillar") was transferred to the TFEU. Its new Title V ("Area of freedom, security and justice") now contains all provisions governing the common justice and home affairs policy (counter-terrorism, policy on border controls, asylum and immigration, police cooperation, judicial cooperation in civil and criminal matters).

An important consequence of integrating justice and home affairs policy in the TFEU is that this key area of EU policy is now largely subject to the regular legislative process and thus to the full co-decision powers of the European Parliament. Legislative acts of the Union adopted on the basis of Title VI of the old TEU are subject to a five-year transitional period starting with the Lisbon Treaty's entry into force: During this period, the Union's system of legal redress has only limited applicability (Art. 10 Protocol (No 36) on transitional provisions, OJ C 83 of 30 March 2010, p. 325 f.).

These changes, especially the end of the pillar structure, also have great significance for data protection. The addition of Art. 16 to the TFEU has created a uniform legal basis for the protection of personal data which applies to all EU policy areas including police and judicial cooperation. Article 16 (1) TFEU has the same wording as the basic right to data protection in Article 8 (1) of the EU Charter of Fundamental Rights (see box for no. 13.1). Article 16 (2) TFEU provides the basis for issuing secondary data protection law concerning the processing of personal data by the institutions,

bodies and other agencies of the European Union and the Member States “when carrying out activities which fall within the scope of Union law”. This has major consequences for data protection with regard to police and judicial cooperation (see no. 13.5).

In addition, with the entry into force of the Lisbon Treaty, the EU Charter of Fundamental Rights (OJ C 83 of 30 March 2010, p. 389 ff.) was promoted to the status of primary law and made binding via a legally binding reference in Art. 6 (1) of the TEU.

Box for no. 13.1

Article 8 of the EU Charter of Fundamental Rights: Protection of personal data

Article 8 of the EU Charter of Fundamental Rights contains the basic right to the protection of personal data. Sub-section 1 guarantees everyone the right to the protection of personal data concerning him or her. According to sub-section 2, these data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Under Article 51 (1) of the Charter, this basic right is binding on the institutions, bodies and other agencies of the Union and on Member States when implementing Union law.

13.2 Amending the European Data Protection Directive

Data protection law is to be modernized at European level as well. The most important part of this effort is revising the legal framework for data protection in the European Union.

Directive 95/46/EC introduced a common legal basis for data protection in the EU Member States already in 1995. After the Lisbon Treaty did away with the pillar structure (see no. 13.1) and due to rapid technological change, the European legal framework for data protection urgently requires a general overhaul. The reform process initiated by the European Commission offers the opportunity to make data protection capable of dealing with the Internet and to bring it into the 21st century everywhere in Europe.

On 9 July 2009, the European Commission launched a consultation procedure on the future legal framework for EU data protection. The results of the consultation are to be incorporated into the European Commission proposal for revising the Data Protection Directive 95/46/EC, announced for the 2nd quarter of 2011.

During the consultation, the Article 29 Working Party and the Working Party on Police and Justice produced a joint paper titled **"The Future of Privacy" (WP 168)** in December 2009. The document contains extensive recommendations to strengthen the principles of data protection, rights of data subjects and the status of national data protection authorities and to expand the EU legal framework to the areas of police and justice.

On 4 November 2010, the European Commission published the communication "A common approach on data protection in the European Union" (COM final 2010 609). In the Commission's view, the dossier contains crucial points for revising Directive 95/46/EC. The communication focuses on the following key points: strengthening the rights of individuals; strengthening the internal market dimension; data protection in the field of police and prosecution authorities; global dimension of data protection; strengthening the data protection authorities.

(The documents referred to can be found on the Internet at http://ec.europa.eu/justice).

The revision of the EU legal framework is very important also for modernizing German data protection law (see no. 1.1), as the former determines the parameters for national regulations and sets binding requirements for lawmakers in the Member States. For this reason, during the consultation process on the Commission's communication and in consultation with the *Länder* data protection commissioners, I submitted a comprehensive strategy for data protection in the European Union. Of crucial importance is the statement that the European legal framework must set a high minimum standard for data protection and at the same time must leave room for more extensive rules to protect data subjects as referred to in Article 8 of the EU Charter of Fundamental Rights. The contribution of the federal and *Länder* data protection commissioners to the consultation is published on my website at www.datenschutz.bund.de, under the heading "Europe and international affairs".

13.3 The Article 29 Data Protection Working Party

The Article 29 Data Protection Working Party adopted important documents during the reporting period. These documents explain key data protection concepts such as "controller" and "applicable law". The document on the future of privacy in Europe should also be noted. The group also conducted a joint enforcement action in the field of preventive data retention and expressed its views on the level of data protection in Andorra, Israel and Uruguay.

The Article 29 Working Party is the central coordinating body for data protection supervision in the European Union. The Working Party comprises representatives of the national data protection supervisory authorities in the Member States, the European Data Protection Supervisor and (as a non-voting member) the European Commission's Directorate D, which also acts as secretariat for the group.

As in previous years, the Article 29 Working Party dealt with a broad range of different topics again in 2009 and 2010. The Working Party adopted a total of 22 working papers during this period. Of these, 16 were adopted as official opinions. The topics dealt with ranged from data protection issues in combating product piracy, the protection of children's personal data and data protection in social networks to the problematic nature of data protection related to RFID chips.

The Article 29 Working Party expressed its position on important data protection issues in the following opinions:

- **The Future of Privacy**: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP 168), adopted 1 December 2009 (see also no. 13.2).

- **Opinion 1/2010 on the concepts of "controller" and "processor"** (WP 169), adopted 16 February 2010. In view of the ongoing development of information and communications technologies (ICT) and the increasingly global nature of data processing, the Article 29 Working Party believes that it is necessary to clarify these terms and distinguish them from the concept of third-party processing. In its analysis, the Working Party came to the conclusion that the distinction between controller and processer remains relevant and that it is necessary "to allocate responsibility in such a way that compliance with data protection rules will be sufficiently ensured in practice". (Regarding rules on third-party processing in the Federal Data Protection Act, see no. 2.4.)

- **Opinion 3/2010 on the principle of accountability** (WP 173), adopted 13 July 2010. Regarding the principle of accountability, the Working Party notes that the processor's responsibility for data protection must be better anchored and implemented in practice. This need is apparent from a number of data protection mishaps. The Working Party therefore put forward a concrete proposal for a principle of accountability which could be included in the revised Data Protection Direction 95/46/EC. This principle of accountability "would require data controllers

to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with and to demonstrate so to supervisory authorities upon request."

- **Opinion 8/2010 on applicable law under Article 4 of the Data Protection Directive** (WP 179), adopted 16 December 2010. In this opinion, the Working Party deals with the "scope of application of Directive 95/46/EC, and in particular of its Article 4, which determines which national data protection law(s) adopted pursuant to the Directive may be applicable to the processing of personal data." In this context, the key terms of Article 4 ("establishment of the controller on the territory of the Member State" and "equipment situated on the territory of the said Member State") are explained in further detail and clarified using appropriate examples. The Article 29 Working Party conducted a joint enforcement action to check compliance with provisions on preventive data retention under Directive 2006/24/EC in all EU Member States during the reporting period. The Working Party found significant differences and shortcomings, especially with regard to the categories of data to be retained, the necessary security measures and the retention periods. The report provides recommendations for action to remedy these shortcomings (WP 172).

For my office, I can report that a staff member in the division for technological data protection has assumed the task of coordinating the technology working group of the Article 29 Working Party. Staff from my office and representatives of the *Länder* data protection commissioners are active in the Working Party's other working groups and are able to include their recommendations and experience.

The website of the Article 29 Working Party has a chronological list of adopted documents, which are available online in all the official EU languages. (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

13.4 Safe Harbour

At the meeting of the Düsseldorf Group in Hanover on 28-29 April 2010, the supreme supervisory authorities for data protection in the private sector reached an important decision on applying the Safe Harbour agreement.

Unfortunately, the experience with the Safe Harbour agreement between the EU and the U.S. has not been entirely positive. I am particularly critical of the fact that, although they have committed to compliance with the Safe Harbour principles, some

U.S. companies active in Europe do not meet the obligations of European data protection law in practice, and that the data protection authorities find working with them very complicated and difficult. This applies in particular to certain “major players” on the Internet (see for example no. 4.1.2).

In their resolution of 28-29 April 2010, the supreme supervisory authorities for the private sector point out that when transferring data to U.S. bodies, data-exporting companies cannot rely on data importers’ declarations that they are certified under the Safe Harbor agreement. Instead, the data exporter must confirm that the certification is still valid. The data exporter must also ask the data importer to demonstrate how it complies with Safe Harbour information requirements with regard to processing the data of data subjects. This minimum check must be documented by the exporting company to present to the supervisory authorities upon request.

The supervisory authorities also emphasize the importance of greater cooperation between the Federal Trade Commission (FTC), which is responsible for enforcing the agreement on the U.S. side, and the European data protection authorities in order to improve compliance with the principles. The data-exporting companies are therefore called on to inform the responsible data protection supervisory authority when they become aware of violations of Safe Harbour principles (see box for no. 13.4).

Box for no. 13.4

Meeting of the Düsseldorf Group in Hanover on 28-29 April 2010

Resolution of the supreme supervisory authorities for data protection in the private sector, adopted in Hanover on 28-29 April 2010
(revised version of 23 August 2010)

Checking self-certification of the data importer under the Safe Harbour agreement by the data exporter

The EU and the U.S. Department of Commerce have had an agreement on the Safe Harbour principles since 26 July 2000.[2] This agreement is intended to guarantee that U.S. companies provide an appropriate level of data protection by agreeing to comply with the Safe Harbour principles. Companies may self-certify by agreeing to comply

[2] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215 of 25 August 2000, p. 7.

with these principles and applying to the FTC. Personal data from Europe may be transferred to U.S. companies certified in this way under the same conditions as within the European Economic Area (EEA). The U.S. Department of Commerce publishes a list of all Safe Harbour-certified companies on the Internet.

As long as the authorities in Europe and the U.S. do not check all the self-certification of U.S. companies, German companies should be obligated to check certain minimum criteria before transferring personal data to U.S. companies on the Safe Harbour list.

In this context, the supreme supervisory authorities for the private sector point out that when transferring data to U.S. bodies, data-exporting companies cannot rely exclusively on data importers' declarations that they are certified under the Safe Harbour agreement. Instead, data exporters must make sure that data importers are Safe Harbour certified and do in fact comply with Safe Harbour principles. At the very least, the exporting company must check whether the importer's Safe Harbour certification is still valid. The data exporter must also ask the data importer to demonstrate how it complies with Safe Harbour information requirements[3] with regard to processing the data of data subjects.

This is important also to enable the importing company to provide this information to persons affected by the data transfer.
This minimum check must be documented by the exporting company to present to the supervisory authorities upon request. Should there be any doubt as to whether the U.S. company complies with the Safe Harbour criteria, the supervisory authorities recommend using standard contract clauses or binding corporate rules to ensure an appropriate level of data protection by the data importer.

When checking, if a data-exporting company finds that the certification of the importing company is no longer valid or that the necessary information for data subjects is not provided, or if other violations of Safe Harbour principles come to light, the responsible data protection supervisory authority should also be informed.

---

[3] Information requirements: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

Cooperation between the FTC and the European data protection authorities plays a key role in improving compliance with the Safe Harbour principles. To this end, the FTC and the European data protection authorities must increase their checking of compliance with the Safe Harbour principles. The legal certainty which the Safe Harbour agreement is supposed to ensure for transatlantic data traffic can be achieved only when the principles are effectively enforced in practice.

13.5 New developments between Stockholm and Lisbon

Many things have happened in the old "third pillar": a new programme with new goals for the EU and above all a new legal framework since the Lisbon Treaty entered into force.

Since my last Annual Report, the framework for what was once known as the EU's "third pillar", i.e. police and judicial cooperation in criminal matters, has fundamentally changed: The Member State governments have set new goals for the further development of the area of freedom, security and justice over the next five years in what is called the Stockholm Programme. This programme has been met with mixed feelings, however (see the resolution of the 78th Conference of Data Protection Commissioners of the Federation and the *Länder*). Although the programme gives data protection a more central position, in view of the planned projects I have my doubts as to whether it will indeed have an impact on the work of the European bodies. In any case, further steps are needed to achieve a balance between security and freedom in Europe (see box for no. 13.5).

Of even more fundamental significance than the Stockholm Programme is the entry into force of the Lisbon Treaty. The previous pillar structure of the EU was dissolved and the exceptional role of the area of police and judicial cooperation in criminal matters was greatly restricted. Although much remains unchanged for the time being, due to transitional arrangements, some changes have already occurred and more are on the way. This is due among others to Article 16 of the Treaty on the Functioning of the European Union (TFEU), which gives the European Parliament and the Council general powers to "lay down the rules relating to the protection of individuals with regard to the processing of personal data" acting in accordance with the ordinary legislative procedure. So unanimity is no longer required, and the European Parliament is a legislative body along with the European governments. Under the Lisbon Treaty, an integral part of this legal framework is also the European Charter of Fundamental Rights, whose Article 8 lists the protection of personal data as one of the key fundamental rights in the EU while stating the conditions for data processing (see no. 13.1 above).

I see this as offering a special opportunity for data protection in the area of the former third pillar. The aim must be both to improve the level of data protection and to achieve greater harmonization of law in Europe. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (see 22nd Annual Report, no. 13.3.1) is thus inadequate in this respect, apart from the fact that it has so far been implemented in very few EU Member States. So the way in which the data protection authorities work together at European level should also be examined. My impression is that the European Commission wishes to act as the engine for modernizing data protection law in the EU, using the new legal framework to thoroughly overhaul the relevant legislation on police cooperation. The Commission has announced this intent several times, most recently in its communication on revising the European Data Protection Directive 95/46/EC of November 2010 (see no. 13.2). The Commission now has the initiative as well as the right to initiate legislation.

At present, the various legislative acts in the area of police and judicial cooperation in criminal matters are difficult even for experts to reconcile. In future, it will therefore be necessary to anchor general data protection principles for this area in legislation. Although special legislation will still be needed to do so (for example regarding the Schengen Information System or Europol), such exceptions to the general principles, for example with regard to the right of data subjects to obtain information from the police, will always require justification and clear expression in law.

Further, the Article 29 Working Party, as European advisory body for data protection issues, needs to be reorganized now that the pillar structure has been discontinued. Limiting the Working Party to the scope of application of Directive 95/46/EC is simply outdated. And the European data protection authorities will have to find a way to coordinate important enforcement tasks more effectively. For this reason, the structure and working methods of the enforcement bodies also need to be reformed. The thoughts on new legislation in the area of police and judicial cooperation in criminal matters are still in the early stages. I will play an active part in the upcoming discussions, and I hope to be able to report further success in my next annual report.

Box for no. 13.5

Resolution of the 78th Conference of Data Protection Commissioners of the Federation and the *Länder* in Berlin on 8 – 9 October 2009.

Shortcomings in European data protection even with the Stockholm Programme

In its Stockholm Programme, the European Union intends to define its policy aims for developing the area of freedom, security and justice in the coming five years. This is the purpose of the draft presented by the Commission of the European Communities.

The Commission's draft mentions protecting personal liberties and privacy as priorities of internal and security policy in a "citizens' Europe", and steps such as the EU's planned accession to the European Convention on Human Rights, information and awareness-raising campaigns on data protection, and the promotion and possible certification of data protection-friendly technologies also point in this direction.

However, specific ideas for improved data protection lag well behind the goals for improved security architecture. For the latter, the Commission's draft contains an extensive catalogue of measures which in some cases are extremely intrusive, such as an electronic system for preauthorizing and recording entry to and exit from Member States and the creation of a European criminal records information system. Without appropriate measures to ensure data protection and security, the plan to create a single platform for information processing offering almost unlimited possibilities for data processing threatens civil liberties.

The data protection commissioners of the Federation and the *Länder* believe further steps are needed to achieve a balance between security and freedom in Europe. Such steps include in particular:

- further developing Council Framework Decision 2008/977/JHA into harmonized data protection legislation which is binding also for national data processing and which ensures a high level of data protection in the area of police and judicial cooperation;

- concluding agreements with third countries subject to their compliance with data protection principles;

- creating an independent data protection advisory and enforcement body for all areas of police and judicial cooperation between the EU Member States;

- evaluating the many security policy projects agreed at EU level with regard to their effectiveness, intrusion on fundamental rights and possible overlaps with each other before adopting further legislative acts;

- improving transparency and democratic controls over legislation in the area of police and judicial cooperation at European level independent of the adoption of the Lisbon Treaty.

The Conference of Data Protection Commissioners of the Federation and the *Länder* call on the Federal Government to support these demands in the subsequent process, also taking into account the Bundesrat's criticism of giving Europol and Eurojust executive powers, for example.

13.6 Selling out to the U.S. on European financial data?

There is some scepticism about the EU - U.S. TFTP Agreement on transferring financial data to the U.S., especially with regard to the involvement of Europol in such transfers.

I have already described my serious reservations about U.S. authorities having access to SWIFT data on money transfers (21st Annual Report, no. 9.4). The U.S. Treasury Department enters these data into the Terrorist Finance Tracking Program (TFTP) to gain insight into the financing of international terrorism and to assist U.S. and foreign intelligence services and law enforcement agencies in preventing and prosecuting terrorism.
In its resolution of 8 – 9 October 2009, the 78th Conference of Data Protection Commissioners of the Federation and the *Länder* spoke out against "selling out to the U.S. on European financial data" and called on the Federal Government to protect the sensitive financial data of its citizens by rejecting any agreement which would allow transferring data well below the threshold of criminal suspicion and which lacks appropriate data protection standards (see box for no. 13.6).

The modified EU – U.S. TFTP agreement which entered into force on 1 August 2010 displays significant shortcomings with regard to data protection.
This agreement gives Europol a key role. Europol is supposed to check whether the U.S. requests asking SWIFT to transfer financial data comply with the requirements and restrictions stated in the agreement. This special monitoring and corrective function was assigned to Europol due to its special expertise. To carry out this role, Europol may require the U.S. authorities to supply additional documents for the exclusive purpose of evaluating the request. SWIFT can respond to U.S. requests

only if Europol determines that the request complies with the terms of the TFTP agreement. So everything ultimately rests on Europol's decision, that is, its interpretation of data protection law.

A major cause for concern is the fact that Europol is supposed to watch over the procedure even though, as a police agency, it also has an interest in transferring the data to the U.S. authorities, because Europol is not allowed direct access to the SWIFT data, but may gain access via the U.S. Further, Europol's new function in practice gives it the power to receive other kinds of data from the U.S. authorities to which it has so far had only limited access. These potential conflicts of interest are not in the interest of the persons concerned or of data protection. It is at least questionable whether Europol can or wants to fulfil the watchdog function it has been assigned by limiting the flow of data; this should be examined soon. For this reason, the Joint Supervisory Authority (JSA), which is responsible for monitoring Europol's data processing (see no. 13.11), has already inspected Europol's checking of U.S. requests. A few days before that inspection, Europol unexpectedly classified the U.S. requests and all related documents as "secret", meaning that the concrete results of the inspection cannot be made public. Further details on the JSA's action were not available at the time this report went to press.

In view of Europol's crucial monitoring function assigned by the European Parliament and the European Commission under the TFTP agreement, these bodies should be informed in detail of the results of the JSA inspection. The same applies to the Council of the European Union, the Europol Management Board and the national parliaments, some of which were very divided over the agreement. This is the only way that any necessary adjustments can be made to the agreement and any misuse be stopped quickly.
Doing so is all the more urgent since the European Commission has already started hearings on introducing an EU TFTP and has given Europol the opportunity to present its data protection monitoring procedures as a model for the new EU TFTP.

Box for no. 13.6

Resolution of the 78th Conference of Data Protection Commissioners of the Federation and the *Länder* in Berlin on 8 – 9 October 2009.

Don't sell out to the U.S. on European financial data!

For counter-terrorism purposes, the U.S. is currently negotiating with the EU on access to data on financial transactions stored on SWIFT servers in Europe, even when these transactions have nothing to do with the U.S. The Conference of Data Protection Commissioners of the Federation and the *Länder* is especially critical of the fact that U.S. authorities seek access to transaction data even in the absence of reasonable suspicion of involvement in or support for terrorist activities. Such an agreement would give U.S. authorities powers that Germany's constitution does not give its own security authorities.

Such an extensive infringement on the right to determine the use of one's own data in the absence of reasonable suspicion of criminal activity would be impossible to justify under data protection law. It would also be highly questionable with regard to the protection of confidence for European enterprises.
Another reason for concern is that data protection standards in the U.S. are significantly lower than those in the European Union. In particular, the U.S. does not have an independent supervisory authority and persons who are not permanent residents of the U.S. have no right to examine the use of their data by U.S. authorities in a court of law.

Further, there are already doubts as to the need for such comprehensive access for foreign authorities to data stored in Europe. For example, within the framework of mutual assistance, law enforcement agencies are already able to transfer personal data in individual cases to investigate suspected terrorist activity.

Finally, it is to be feared that such an agreement on access to SWIFT data may set a precedent. Firstly, the U.S. could use the same arguments to demand access to other sensitive data stored in Europe, such as telecommunications data. Secondly, after giving the U.S. such broad access to European data, it would be difficult for the EU to justify denying such access to other third countries.

The Conference expects the Federal Government to protect individuals' sensitive financial data effectively and to reject an agreement which would allow transferring data well below the threshold of criminal suspicion and which lacks appropriate data protection standards.

13.7 Checking data against lists of terrorists

Again in this reporting period, I have found myself dealing with the UN and EU terrorist lists. It is still not clear who may or must check customer and employee data against these lists, in which situations and on which legal basis.

Questions about the usefulness and lawfulness of these lists of terrorists and terrorist organizations (UN Al-Qaida Sanctions List, EU list of terrorists and terrorist groups) and about the practical consequences for persons on these lists occupied me already in my previous annual report (see 22nd Annual Report, no. 13.6). Although some action has been taken in the meantime, basic questions remain unresolved.

Apart from the lack of evidence that the lists even make a significant contribution to counter-terrorism, the amendment to the relevant regulation in response to major criticism from the European Court of Justice has somewhat improved the legal situation for persons on the lists. According to Council Regulation (EU) 1286/2009 of 22 December 2009 (OJ L 346 of 23 December 2009), the consultations for which I participated in at national level via Germany's Federal Foreign Office, listed persons are now to be informed by the European Commission of the reason for their listing and to be given the opportunity to express their views on the listing. These are then forwarded to the UN Sanctions Committee. What this committee does with this information, however, remains as opaque as its own listing procedure.

The discussion has increasingly focused on the question as to who is authorized and obligated, and in which situations and on what legal basis, to use these lists in screening. The wording of the Regulation fails to make this clear; it states only that "No funds or economic resources shall be made available, directly or indirectly, to, or for the benefit of, natural or legal persons, entities, bodies or groups listed" (Article 2 (2) Regulation (EC) No 881/2002).
In terms of their wording, this and a similar provision are addressed to anyone. In practical terms, they leave companies in particular with the question whether they must check their employees against the lists or accept it when others do.

In addition, an exception applies in the case of customs law: As I found out after receiving numerous comments from affected businesses, customs authorities now require all employee data to be checked against the terrorist lists before granting the status of Authorized Economic Operator (AEO). I have reservations about that. I find no provisions in the relevant Commission Regulation (EC) No 1875/2006 laying down provisions for the implementation of the Community Customs Code nor in the more detailed European Commission guidelines (TAXUD 2006/1450) which would justify

such systematic checking of all employees as part of the certification procedure under customs law. I have informed the Federal Ministry of Finance about my concerns regarding this practice by the customs authorities and the AEO service instruction on which it is based.

In response, the Federal Ministry of Finance revised the AEO service instruction to clarify that employee data should be checked against the EU list of terrorists only for employees active in “security-relevant areas” (see AEO service instruction, last revised 22 June 2010, 253). As a result, customs officers may no longer require the systematic checking of all employee data as part of the AEO certification process. Although this revision resolves my concerns on a central point, I still recommend creating an explicit legal provision on the extent of data checking permitted in the framework of AEO certification, because I hear from practitioners that different customs offices interpret the service instruction very differently.

The need for a legal provision is apparent, also in view of the principle of proportionality, from the fact that the group of employees in security-relevant areas can be defined very differently. The more employees defined as part of this group, the more will be subject to data screening and the more such screening resembles universal employee data screening which is problematic in terms of data protection. In order to create legal certainty for the companies concerned, I recommend legislation defining the type and extent of organizational measures companies must take to satisfy the requirement of due diligence. Due to the European dimension of the questions associated with AEO certification, the Federal Government should work at European level to clarify the relevant EU customs rules.

Due to the uncertainty of companies and associations with regard to this issue, I have asked the Federal Government for a statement on its position. After checking with the other ministries, the Federal Foreign Office informed me that companies and other economic operators are not legally obligated to conduct systematic screening of all their customer and employee data; instead, they are required to conduct such screening to the extent required for due diligence, and anything beyond that would violate the principle of proportionality.
I regard this statement from the Federal Foreign Office as a step in the right direction, although I fear that companies will continue to be uncertain as to what the law requires.

Because the discussions of a possible legal obligation to conduct data screening and the resulting legal uncertainty stem from European law, I have also asked the

European Commission for clarification on interpreting the counter-terrorism regulations. I am still waiting for a response.

In the meantime, various parties have proposed setting up a round table to give all stakeholders an opportunity to express their views of the problem and to seek a common solution. I am open to such a proposal.

13.8 A new framework agreement with the U.S.

For years, there has been criticism of the way U.S. authorities handle the data of European citizens. The EU now hopes that a new agreement with the U.S. for the area of police and judicial cooperation in criminal matters will set binding data protection standards at the same level as in Europe.

It has almost become a commonplace that the U.S. has a completely different understanding of data protection. Criticism of the U.S. was everywhere in the past, whether over the transfer of passenger name records (see no. 13.9), financial transaction data (see no. 13.6) or fingerprint and DNA reference data (see 22nd Annual Report, no. 13.4). Criticism focused on excessive data retention periods, the lack of independent data protection supervision, and the lack of legal redress for European citizens, to mention only a few points.

So I welcome the fact that in early December 2010, the European ministers of justice and home affairs gave the European Commission a mandate to start negotiating a framework agreement with the U.S. This agreement is supposed to define the principles to be applied by the security authorities on both sides of the Atlantic when transferring and processing data.

Out of a lengthy catalogue of demands by the European data protection commissioners, I would like to focus on a few especially important ones:

- In order to achieve a consistently high standard of data protection, the standards to be negotiated should apply not only to future agreements between the EU and the U.S., but also to existing ones. It is equally important that the new standards be applied when individual Member States transfer data to the U.S. on the basis of national law or bilateral agreements, whether these agreements or the national legal basis already exist or not.

- European citizens must be able to enforce their data protection rights in the U.S. against authorities and courts. This is currently in doubt. The agreement offers a chance to dispel these doubts with clear rules which are binding for all U.S. authorities and courts and apply regardless of the nationality of the data subject.

- The practice of U.S. security authorities of storing data for decades (without reasonable suspicion of wrongdoing) is simply incompatible with the European understanding of data protection. Such data retention is excessive and must be appropriately limited.

- An independent supervisory authority is also integral to the basic European understanding of data protection and is anchored in both Council of Europe Convention 108 and the EC Data Protection Directive. The European Court of Justice once again emphasized this in a recent ruling (see no. 2.1).

The negotiations are likely to be long and difficult for a number of reasons, but the chance of achieving binding data protection standards for sharing personal data with the U.S. is worth the effort.

13.9 Airline passenger data

The use of airline passenger data to prevent and combat terrorism and serious crime remains highly topical.

My last annual report already dealt with the use of passenger data (see 22nd Annual Report, no. 13.5), and the issue remains topical: In September 2010, the European Commission issued a communication on a "global approach" to concluding agreements on airline passenger data (passenger name record (PNR) data). The European Parliament also caused some movement, as, according to the Lisbon Treaty, it must approve agreements with third countries. These are now being re-negotiated (see no. 13.8.1). As a result, the Council has held off on considering whether to process PNR data of passengers travelling between the EU and a third country and use these data also within the EU. The European Commission has announced that it will present a new legislative proposal in early 2011. The Federal Government has also presented draft legislation requiring airlines to provide passenger data to the customs authorities on request. Ministerial consultations on this proposal, which is not intended to transpose European law, had not yet been completed when this report went to press (see no. 13.8.2).

13.9.1 New developments in agreements with third countries on airline passenger data

The existing agreements on the transfer of passenger data are being re-negotiated. The European Parliament will play a decisive role in this process, as its approval is now necessary under the Lisbon Treaty.

I continue to have serious reservations about the undifferentiated transfer and use of airline passenger data without reasonable suspicion for threat prevention and law enforcement purposes. This involves systematically extracting passenger data from airline reservations systems, transmitting them to other countries, where they are not adequately protected and often retained for unreasonably long periods of time – all without reasonable suspicion or any indication that processing these data for threat prevention and law enforcement purposes is even useful or necessary.

I have repeatedly pointed out the particular inadequacies of the PNR agreement with the U.S. (see 22nd Annual Report, no. 13.5). In one of the main points of criticism, the transmission procedure chosen, the shortcomings have not yet been remedied: The American authorities continue to insist on online access to the airline reservation systems (“pull system”), although the agreement specifies a transition by 1 January 2008 at the latest to a "push" system in which the airlines themselves transfer the data to the U.S. I view this as a violation of the agreement and expect the European Commission and Council to insist that the U.S. authorities comply with the transition as agreed.

In September 2010, the European Commission issued both a communication on the future “global approach” to PNR agreements and guidelines for negotiations with the U.S., Australia and Canada on new PNR agreements. The Commission understands the “global approach” to be a set of general criteria to be applied to all future PNR agreements with third countries. In an opinion, the Article 29 Working Party welcomed the global approach to PNR agreements and its efforts on behalf of improved data protection in the agreements. However, the Working Party continued to question the need for security authorities to process passenger data and expressed serious reservations about referring to “risk assessments” and “analysis of patterns” based on PNR data. It also called for further improving privacy protection for passengers. The European Parliament expressed many of the same concerns and demands - and the European Parliament will be the key in future, because the Lisbon Treaty requires the approval of the European Parliament to adopt new treaties (see no. 13.1). This includes the PNR agreement with the U.S., which will expire in 2014 at the latest. The newly strengthened role of the European Parliament

represents a chance to improve data protection in transatlantic data traffic. I hope the members of the European Parliament know how to use their power.

13.9.2 Will customs authorities soon have access to passenger data too?

The Federal Ministry of Finance wants to grant the Customs Administration extensive access to passenger data. I am critical of this development.

Recently, demands have repeatedly been made to transfer passenger data to additional authorities beyond those required by European law. For example, the Federal Ministry of Finance has presented proposed legislation to create a legal basis for gathering and transferring passenger data to Customs Administration authorities and the Customs Investigation Service. The proposed legislation would give the customs authorities even greater access to passenger data than the Federal Police, for example, whose powers of access are determined by EU law (Directive 2004/82/EC; see 22nd Annual Report, no. 13.5.2). For example, they would also have access to data of passengers of flights from Germany to non-EU countries and even to data of passengers on flights within the EU. The proposal also provides for transferring information about the payment of booked flights to the customs authorities and for extensive options for forwarding the data to other authorities.

I am critical of this development. Apart from my fundamental reservations about forwarding passenger data without reasonable suspicion and for different purposes, I am also concerned by the fact that the draft legislation would allow detailed personal data on airline passengers to be transferred not only to the customs authorities, but also to other government agencies. These data could be used to create profiles or patterns of passenger travel. This should be viewed all the more critically, as the draft legislation would also cover data of passengers travelling between Schengen countries, even though checks of persons travelling within the Schengen area have largely been discontinued.

The ministerial consultations, to which I was invited only at a later phase, were not yet completed when this report went to press. I hope the Federal Government decides to stop this project.

13.10 Implementing the “Swedish Initiative”

The same conditions should apply to data transfer between European and national police authorities. But the basic problem remains: Europe does not have a consistently high level of data protection in the field of law enforcement.

According to the “Swedish Initiative”, the transfer of personal data between police in different EU Member States should not have to satisfy requirements any stricter than those that apply to data transfers between police within an EU Member State. This may sound plausible in a united Europe, but it depends on a similarly high level of data protection in all EU Member States. However, this is still not the case.

For this reason, in their resolution of 6 – 7 November 2008 (22nd Annual Report, no. 13.3.6), the data protection commissioners of the Federation and the *Länder* called on German lawmakers to utilize the remaining room for discretion in implementing the Swedish Initiative to improve data protection. Following a lengthy delay, the Federal Government has now introduced a legislative proposal, which was still in the early stages of the legislative process when this report went to press. This proposal, which underwent numerous changes in the drafting process, appropriately addresses most of these concerns. During the ministerial consultations, I successfully advocated for clarification of the conditions under which data transfer may take place and when it is prohibited, and for limiting the scope of information provided without a previous request. I see the remaining shortcomings as consisting primarily in the fact that the conditions for police sharing of data are to be improved, while the rights of individuals vis-à-vis the police are not to be strengthened at the same time. So I have high hopes that the Lisbon Treaty will bring a fresh start also in this area (see no. 13.5).

13.11 Europol

13.11.1 Europol: Central office for police information-sharing in the EU

Europol is increasingly becoming a European central office for police investigation with extensive data collections. However, this is permitted only within the Council Decision establishing Europol.

Over the years, Europol has steadily increased in importance. The Council Decision establishing Europol entered into force on 1 January 2010, giving Europol a new legal basis and expanding its tasks and powers (see 22nd Annual Report, no. 13.3.3). The Lisbon Treaty has now defined Europol’s tasks in primary law: in Article 88 of the Treaty on the Functioning of the European Union (TFEU) which explicitly assigns Europol the mission of strengthening action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating crime. As a result, the Member State governments have undertaken in the Stockholm Programme (see no. 13.5 above), which sets out the

policy goals for the further development of the area of freedom, security and justice, to make greater use of Europol's potential by having it play a greater role in the mutual exchange of information.
Europol is therefore striving to position itself as the central office for information-sharing by the police in the EU. To get there, it has started a number of projects; Europol's Joint Supervisory Body, comprised of representatives from the Member States' data protection authorities, is responsible for determining whether these projects are permitted under data protection law. The projects include the following:

- "Check the Web" (adopted in 2007 by the EU Justice and Home Affairs Council) to increase cooperation between the police and judicial authorities in monitoring and analysing publicly accessible Internet sources. The core component of the project was setting up an information portal at Europol as a technical platform for Member States' security authorities to exchange information. Over time, however, Europol started using this portal to enter its own information and to create its own analyses using the information from the portal, which increasingly became a Europol information system. At the recommendation of the Europol Joint Supervisory Body, the portal was therefore transferred to the legal framework of the Europol Council Decision (2009/371/JHA) and is now run as an analysis work file as referred to in the Council Decision.

- Under the heading "cross-matching", Europol examines the possibility of expanding its information collection by checking its own information against Member State information exchanged via Europol. Europol plans in future steps to check data from European information systems and the Member States' national police information systems. Currently, Europol is checking only data transferred to it by the Member States without further specification to see whether it has jurisdiction and whether it already has information on the matter in its own information systems. Although the current practice may still comply with the relevant provisions of the Europol Council Decision, it is doubtful whether the future development phases can be carried out lawfully without amending the Decision.

- The Council Decision also authorizes Europol to gather personal data from private, commercial information providers, such as credit rating agencies. Given the large quantity of personal data such credit rating agencies collect on innocent persons, Europol is allowed access to such data only to the degree absolutely necessary to carry out its tasks. Whether the Europol Council Decision provides a sufficiently precise legal framework remains to be seen.

As these examples demonstrate, it is often questionable whether Europol's striving to become an information hub for police investigative cooperation in Europe and the measures taken to that end can be put into practice on the basis of the current Europol Council Decision. These measures are often new, more intrusive forms of data processing which would require special legislation which adequately specifies and limits their content, purpose and extent.

Against the backdrop of Europol's growing importance, the question also arises whether the current structure of data supervision as performed by the Joint Supervisory Body involving all 27 EU Member States is still capable of ensuring effective, efficient and flexible data protection oversight.

13.11.2 Complaints from Germany to Europol's Appeals Committee

For the first time in its existence, Europol's Appeals Committee had to decide on two queries from Germany. They had to do with the extent of the right to information.

The Europol Convention and Council Decision establishing Europol assigned Europol's Joint Supervisory Body the task of dealing with requests from individual data subjects for Europol for information about their personal data on file and to correct or delete such information. For this purpose, the Joint Supervisory Body set up its Appeals Committee as a kind of court to provide legal remedy for individuals claiming the right to information about their personal data and the right to have Europol correct or delete these data.
For the first time, the Appeals Committee had two such claims from Germany. The applicants each objected to the fact that, as they claimed, Europol had failed to make clear in its notification to them whether it had data about them in its databases. Because the applications were submitted in 2009, the Appeals Committee was required to deal with them in accordance with the relevant provisions of the Europol Convention (rather than the Council Decision, which went into effect in 2010). Under Article 19 (3) of this Convention, "the right of any individual to have access to data relating to him or to have such data checked shall be exercised in accordance with the law of the Member State where the right is claimed". Article 19 also lists reasons for refusing such access. Since the applicants claimed their right to access in Germany, German law applied, specifically: Article 19 of the Federal Data Protection Act. Applicants are also to be informed when no data related to them are stored by the controller. This follows directly from the basic right to determine the use of one's own data. Determining the use of one's own data requires the freedom to decide

whether to claim the right to delete or correct data and the right to effective legal protection. This requires knowing not only who processed which data for which purposes, but also knowing that none of one's personal data are recorded. Notification which fails to make this clear fails to fulfil the constitutionally mandated protective function of the right to information. Information (including the information that none of one's personal data have been recorded) may be withheld only if one of the conditions specified in Section 19 (4) of the Federal Data Protection Act applies. Article 19 of the Europol Convention contains a similar provision on refusing to provide information. As a result, the Appeals Committee must decide whether Europol's notification in the two cases complied with the relevant provisions of the Europol Convention and the Federal Data Protection Act. The appeals are still being processed.

13.12 International organizations

During the reporting period, both the Council of Europe and the Organization for Economic Cooperation and Development (OECD) were occupied with important individual issues and with preparing comprehensive amendments to their data protection instruments.

In November 2010, the Council of Europe adopted an important recommendation on profiling, to be implemented by its member states at national level. The collecting and compiling of personal data to create profiles represents a special threat to individuals' right to control the use of their personal data and should be strictly regulated to protect individual privacy. The recommendation aims to "strike a fair balance" between data protection and legitimate interests justifying the creation of profiles. With regard to data protection, the Council of Europe will focus on updating its 1981 Convention 108 for the protection of individuals with regard to automatic processing of personal data. The planned revision of the Convention, which is to start in spring 2011 with a consultation, is intended particularly to confront new challenges arising from technological advances on the Internet, such as cloud computing and social media. The modernization efforts thus are very similar to those being considered at EU level (see no. 13.2) and in Germany (see no. 1.2).

In 2010, the OECD celebrated the 30th anniversary of its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data with three events focusing on the significance of the Guidelines, the role of individuals and the economic dimension of data protection. Based on the results of a survey of its member states to be conducted in early 2011, the OECD will decide whether to revise the Guidelines. In addition, the OECD has continued its efforts to improve

cooperation between the national data protection authorities. It has drawn up an overview of national points of contact and a standard form to facilitate contact between data protection authorities, and it supports the work of the Global Privacy Enforcement Network (see no. 4.11) by developing the network's website.

13.13 European Privacy and Data Protection Commissioners' Conference

During the reporting period, the European Privacy and Data Protection Commissioners' Conference focused on issues related to police and judicial cooperation in criminal matters.

The European Privacy and Data Protection Commissioners' Conference was held in Edinburgh on 23 – 24 April 2009 at the invitation of the UK Information Commissioner's Office. The conference adopted a declaration recalling the data protection authorities' commitment to maintaining a high level of data protection and stressing that Europe must continue to act as a global leader in promoting data protection (see Annex 7). In another resolution, the conference called on the European countries to ensure that applicable data protection standards are met when concluding international agreements on police and judicial cooperation in criminal matters (see Annex 8).

Issues related to police and judicial cooperation in criminal matters at the European Privacy and Data Protection Commissioners' Conference in Prague on 29 – 30 April 2010. In a resolution on the planned agreement between the EU and the U.S. concerning data protection standards in the area of police and judicial cooperation in criminal matters (see no. 13.8 above), the conference called on the EU to insist on a high level of data protection (see Annex 9). In a resolution on the use of body scanners for aviation security, the conference stressed the need to find a fair balance between the effectiveness and need for this new technology and its impact on privacy (see Annex 10).

13.14 International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners kicked off key initiatives for creating international data protection standards and improving global cooperation.

The 31st International Conference of Data Protection and Privacy Commissioners, held in Madrid on 4-6 November 2009, had a record number of participants: More

than a thousand data protection and privacy commissioners from more than 80 countries gathered to discuss current issues of privacy protection. The main focus of the event was improving and increasing international cooperation. Special attention is to be given to international data protection standards to be developed jointly with industry representatives and non-governmental organizations, and intended to lay the groundwork for an international data protection convention (see Annex 11).

The 32nd International Conference of Data Protection and Privacy Commissioners was held in Jerusalem on 27 – 29 October 2010, hosted by ILITA, the Israeli Law, Information and Technology Authority, with the motto "Privacy: Generations". Intensive discussions dealt with the generational differences in data protection requirements, using the example of social media such as Facebook and Twitter. Another focus was current challenges to data protection posed by new technologies. In this context, the conference adopted a resolution on privacy by design calling for data protection to be incorporated into the design of information technology systems from the earliest stages.

15 Important items from past annual reports

1. 22nd Annual Report, no. 5.7: **Establishing a visa alert database**

   Following the announcement in the coalition agreement for the 17th legislative term, the Federal Ministry of the Interior presented a ministerial draft on creating a central visa alert database. Although the plan from the previous legislative period to store data on all visa applicants' hosts, persons submitting formal obligations and other references without reasonable suspicion was discontinued, some of the reasons for alerts to be stored in the database go beyond what is absolutely necessary, for example storing data when unlawful behaviour is suspected rather than proved. I am also critical of the fact that crimes are to be entered into the database which are unrelated to the visa process or other foreign matters. Further, according to the draft, the security authorities are to have extensive access rights. As part of my participation in the interministerial coordination process, I clearly expressed my reservations about the planned design of the visa alert database. If this project is pursued, it should first of all assist the German visa authorities in their work. The data entered into the database should be

oriented exclusively on this purpose. It remains to be seen how this project is implemented.

3. 22nd Annual Report, no. 10.5.1: **Collecting migration statistics on job seekers**

   I reported on the new provision in Section 281 (2) of the Social Code, Book III, on collecting information about the immigrant background of job seekers for statistical purposes only. The relevant statutory instrument entered into force in October 2010 (Federal Law Gazette 2010 I, p. 1372). It also provides for distinguishing ethnic German resettlers. I find the legislative intent to collect precise statistics concerning this group also with regard to labour market participation and basic subsistence in order to promote integration reasonable.

   The plans to use the data on immigrant background also in daily operations were unsuccessful in the previous legislative term and have not yet been revived.

4. 22nd Annual Report, no. 14.2: **Data protection at German diplomatic missions abroad**

   The data protection shortcomings found during an inspection and advisory visit to a German diplomatic mission abroad have since largely been remedied by the Federal Foreign Office. With regard to the unresolved issue of the lack of a directory to the data processing systems, the Federal Foreign Office has informed me that it is currently working on including such a directory in a new system of forms. Also in need of discussion is the security of communications between the legal and consular departments abroad and the German authorities via the Internet. Because the main issue here is communications between state and local authorities (e.g. registration offices), I have included the *Land* commissioners for data protection in the discussion. The consultations had not yet been concluded when this report went to press.

8. 22nd Annual Report, no. 3.4.1: **European Services Directive (use of the European Internal Market Information System (IMI))**

   Directive 2006/123/EC on services in the internal market was implemented on 28 December 2009. In the *Länder*, the “points of single contact” are available to advise potential service providers.

And the Internal Market Information System (IMI) was launched in early 2010, enabling many local, regional and national authorities to communicate with their counterparts abroad, for example in case of doubt that documents presented by a service provider are authentic, so that it is necessary to consult the responsible authorities in the issuing Member State.

The federal and *Länder* data protection commissioners and the European Data Protection Supervisor have all demanded that IMI be operated in accordance with a clear legal basis; the European Commission has so far not met this demand, although it has promised to do so.

As expected, the number of enquiries made using IMI is not very large, so that in the meantime, there are thoughts of using the existing technical infrastructure also for enquiries at exclusively national level. Not only is there no legal basis for using IMI within a Member State, but doing so would also lead to enormous problems for other reasons. The central server of the European Commission is located in Luxembourg, so every national-level enquiry would also constitute cross-border European data transfer. Another problem is that the Commission has so far refused to allow the *Länder* data protection commissioners, who are responsible for the prior checking of IMI implementation and its national use, access to the security strategy and the technical description of processes on which IMI is based. The Commission does not want to provide this information, arguing that the system is subject only to inspection by the European Data Protection Supervisor. I will continue to monitor the situation.

9. 22nd Annual Report, no. 10.1: **Act on Genetic Testing: Setting limits for genetic tests**

The Act on Genetic Testing in Humans, which entered into force on 1 February 2010, governs genetic testing and analysis as well as the use of the resulting genetic samples. The Act contains numerous data protection provisions such as the right to be informed of the results of genetic tests as well as the right not to be informed if one does not wish to know the results.

Key provisions govern paternity tests, which are allowed only with the consent of the person to be tested. Secret paternity tests are not permitted. Only a doctor may conduct genetic tests for medical purposes. If the test is a predictor of one’s own health or that of an unborn child, then genetic advising must be provided before or after the test.

Labour law prohibits all genetic testing at the request of the employer. Genetic tests may be permitted only under strict conditions and in the framework of occupational health and safety.

Insurance companies cannot require genetic testing or the results of previous testing before or after issuing an insurance policy. To prevent abuse, there are narrowly defined exceptions when issuing policies for life, occupational disability, disability or long-term care insurance with a certain high level of benefits.

Unfortunately, the Act does not contain provisions on data protection for genetic testing in the field of research. This is very regrettable, because of the high level of legal uncertainty among all involved in this field.