24th Activity Report of the
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
covering the years 2011 and 2012

(Excerpt)

Contents

Introduction

The reporting period was marked by the long-overdue discussion of the further developing of data protection. The most significant impetus was provided by the European Commission with its proposed legislation for modern, Europe-wide data protection.

Unfortunately, despite repeated announcements by the Federal Government, Germany's elected officials did not take on the overdue task of updating data protection law. It is especially regrettable that efforts to improve the protection of employees' data, which I reported on already two years ago, also failed to make progress. At the same time, attempts by individual data protection supervisory authorities to force globally active Internet companies to comply with data protection law have quickly proved limited. This national vacuum can be filled only at European level.

Even though the European Commission's proposals need further improvement and discussion, this project is very ambitious and important. In view of the global flow of data, personal data can be protected effectively only if the laws are harmonized at least at European level, cross-border coordination of data protection supervision is improved and more effective sanctions are enforced in case of violations.

Since the Lisbon Treaty entered into force, data protection has been a fundamental European right. This is why it is logical for the EU data protection package to cover both the private and the public sector. In addition to the proposed General Data Protection Regulation, a separate directive is intended to guarantee data protection by police and judicial authorities. When this directive will be implemented into German law, it must continue to meet the requirements formulated by the Federal Constitutional Court.

But legislation alone is not enough to guarantee the fundamental right of data protection; technical requirements, i.e. privacy by design and privacy by default, are more necessary than ever, as are procedural safety measures, such as data protection impact assessments and seals of quality. This is where industry must act, especially since compiling and analysing personal data – "Big Data" – offers enormous commercial potential.

Powerful representatives of industry and government from third countries are adding their voices to the European discussion of data protection, predicting dramatic economic disadvantages if the level of European data protection will be raised as planned. I find it difficult to follow these arguments, especially the demand, made mainly by industry representatives, to “streamline” data protection law by excluding supposedly non-sensitive data. As the Federal Constitutional Court found already many years ago, in an age of automated data processing, no personal data can, by their nature, be non-sensitive. This finding remains true up until today. So I was pleased that the 69th German Jurists Forum in 2012 rejected demands to water down data protection.

Data protection has always reacted to the challenges of technology. Making information technology conform to social values continues to be the goal of data protection. I see no reason why our society should relinquish this goal in the Internet age and should unconditionally surrender to supposed technical or economic constraints.

The figures for 2011/2012 are also impressive: 9,729 citizens submitted requests for my assistance. My 85 staff members conducted 106 inspections, in which I was required to lodge 15 complaints.

During this reporting period as well, data protection found broad support, for which I am grateful. I would like to convey special thanks to the members of the German Bundestag of all parties and to other representatives of the public and private sectors who worked on behalf of data protection. I would also like to thank private individuals who pointed out problems, thereby helping to improve data protection practice. Finally, I would like to very much thank my staff, whose commitment has significantly helped strengthen data protection.

Peter Schaar

1 Summary of all the recommendations

I recommend that the Federal Government should ensure a high level of protection for basic rights with regard to the European Investigation Order (EIO) (cf. no.2.2.1).

I recommend that the Federal Government should remain committed to improving data protection law in the framework of consultations on the EU regulation on electronic identification and trust services (cf. no. 2.3.4).

The requirements in the ruling of the European Court of Justice on the independence of the Austrian data protection commission must also be implemented for the Federal Commissioner for Data Protection and Freedom of Information (cf. no. 3.1).

The use of video monitoring technology by the federal administration must be made data protection compliant (cf. no. 3.3.1).

The data protection foundation Stiftung Datenschutz should be redesigned so that it can carry out its tasks effectively and truly independently (cf. no. 3.6).

I recommend that the Federal Government should consider the data protection law aspects of individual processes at an early stage when seeking ways to optimize the exchange of social insurance data (cf. no. 4.2.1).

The Federal Court of Justice decision on the conditions of the right of access under Section 101 of the Copyright Act is likely to result in more customer data being sent from Internet access providers to right holders. Because the right of access should be limited to serious violations of the law, I recommend that legislators review the current law and amend it with the principle of proportionality in mind (cf. no. 5.2).

When using cloud services, processors should select cloud service providers carefully, specify details of data protection and data security and determine the countries in which data are stored and processed. In particular, before entering the cloud (sensitive) personal data should be encrypted under the sole control of the processor according to the state of the art (cf. no. 5.3).

I recommend that the Federal Government should review security authorities' powers of intervention at regular intervals to check their effectiveness, necessity and proportionality (cf. no. 7.1.).

I recommend that legislators should grant security authorities new powers only on the basis of a comprehensive evalutation based on the guidelines for conducting ex-post evaluation of the law with special attention to consequences under data protection law (cf. no. 7.1).

I recommend that legislators should thoroughly evaluate the Act on the Counter-Terrorism Database, remedy its shortcomings (cf. no. 7.2) and draw conclusions applicable to the Act on a Database of Right-Wing Extremism (cf. no. 7.3).

I recommend that, in the Act to Improve the Fight Against Right-Wing Extremism, legislators should design sufficiently specific and proportional provisions to protect innocent persons (cf. 7.3).

I recommend that the Federal Government, when describing standard services for developing software to intercept telecommunications at the source and carry out other intrusive measures, should establish clear rules for the functioning of the software and should make sure that in particular the source code is unconditionally available to the data protection authorities for purposes of inspection (cf. no. 7.4.1).

I recommend that the Federal Government, when developing the Police Information and Analysis Network, should comply with central tenets of data protection law and should store so-called person-related hints in the INPOL system only on the basis of clearly defined criteria (cf. 7.4.5).

I recommend that, when posting public appeals on the Internet and in social networks, the federal police authorities should pay attention to the special nature of these media and should follow the outline developed by the conference of federal and state data protection commissioners (cf. no. 7.4.7).

I recommend that the Federal Government should soon thoroughly evaluate the practice of Authorized Economic Operator (AEO) certification (no. 7.5.1).

I recommend that legislators should undertake the reform of the security authorities needed in the light of the NSU terrorist case only after a thorough and

comprehensive investigation of the causes and faulty developments, and should adequately respond to the need for efficient monitoring the intelligence services (cf. no. 7.7.6).

I recommend that legislators should create the necessary legal basis in the Act on Federal Civil Servants to enable research projects so that the Nazi past of federal ministry staff can be carried out on adequate legal footing (cf. no. 8.6).

I recommend that legislators should address the issuing of new tax identification numbers in case of special risks as to data protection (such as witness protection, adoption, sex change) (cf. no. 9.2).

I recommend that, in shifting from paper to electronic wage tax cards, the tax administration should take the necessary technical and organizational measures to prevent unauthorized access to electronic data stored in the central database as far as possible (cf. no. 16.6; recommendation repeated from the 23rd Report, no. 9.3).

In setting data protection standards for smart energy grids, the Federal Government should set a high standard in particular in the Data Protection Ordinance under the Energy Industry Act, taking into account the principles of purpose limitation, data minimization and necessity (cf. no. 10.1).

Legislators should follow the recommendation of the Petitions Committee of the German Bundestag and in Section 35 (2) second sentence no. 4 of the Federal Data Protection Act (storage of data related to credit ratings) make the time limit start with the first day these data are stored (cf. no. 10.2).

I recommend that the statutory health insurance funds should not increase competition in the health-care sector at the cost of data protection and the privacy of insured persons (cf. no. 11.1.1).

I recommend that the statutory health insurance funds should respect the collection of data reserved to the Health Insurance Medical Service (MDK) and not undermine its competences (cf. nos. 11.1.6 and 11.1.7).

I recommend that in Section 200 of Book VII of the Social Code, legislators should clarify the definition of “expert opinion” in the statutory health insurance (cf. no. 11.4.1).

I recommend that legislators should address the issue of data protection of employees again in the next legislative term and create relevant legislation which effectively restricts registration and surveillance in the workplace (cf. no. 13.1).

I recommend that legislators anchor within the German Fiscal Code data subjects' rights to have access to their data (cf. no. 16.7).

2 Data protection at European and international level

Data protection is less and less able to meet, with national instruments alone, the challenges posed by the globalization of information processing. This is true not only in regard to current projects to modernize data protection at European level. Key developments in regard to data protection at European and international level will be addressed in the following.

2.1 Brussels' great achievement: The reform of European data protection law

On 25 January 2012 the European Commission initiated a comprehensive reform of European data protection law which gave new – and from now on Europe-wide – momentum to the debate on modernizing data protection legislation.

The reform package the Commission has put forward comprises three elements:

– A Communication from the Commission on "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century", COM(2012) 9 final

– A Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final

– A Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final

The Communication from the European Commission details the need to reform existing European data protection legislation and substantiates the basic conclusions it draws from that in the drafts of two legal acts. The General Data Protection Regulation covers the processing of personal data by both non-public and public agencies, excluding the police and judiciary (cf. no. 2.1.1). The Proposal for a Directive is intended to regulate data protection in the areas of police and justice (cf. no. 2.1.2).

The ambitious programme of reforms primarily serves to develop existing European data protection law (which essentially dates back to 1995) and to adapt it to the challenges faced by data processing in the 21st century. As a whole, I feel positively towards the European Commission's initiative, since it combines the intent to modernize data protection legislation with the Europe-wide harmonization of that legislation at a notable level.

Since the Commission put forward the Proposals they have been the subject of quite intense debate in the Council of the European Union (comprising the governments of the Member States) and in the European Parliament in the context of the legislative procedure. The Council working group responsible for data protection, the Working Party on Information Exchange and Data Protection (DAPIX), held numerous meetings to discuss the package of reforms, initially under the Danish and then under the Cypriot Presidency. Germany is represented by the Federal Ministry of the Interior (*Bundesministerium des Innern* (BMI)) in DAPIX. I had the opportunity to attend the DAPIX consultations at working level. Prior to the DAPIX meetings the Federal Government's positions are coordinated at national level, a process I have also been involved in.

In recent months it has become clear that the BMI takes a considerably more critical stance on the reform proposals than I do. For instance, the tried and tested system and regulatory structure applied to data protection law (e.g. a prohibition with authorization proviso or taking the term "personal data" as the point of reference in data protection law) are called into question both in the public debate and in negotiations within the Council. Such fundamental issues need to and must be discussed. Nevertheless, it is surprising that they were not introduced to the debate until concrete proposals for a reform were put forward at European level following a ten-year deadlock at national level.

The rapporteurs in the competent LIBE (Civil Liberties, Justice and Home Affairs) committee in the European Parliament submitted their first comments together with proposals for amendments in January 2013.

Aside from the formal legislative procedure at European level, an intense and wide-ranging public debate on the reform package has also developed. Data protection authorities, the private sector, academia, public administration and civil society are bringing their ideas and analyses to bear in that debate. It is evidently generally acknowledged that the new European data protection law will set the legal framework for the coming years. The not inconsiderable efforts which businesses, lobby groups and government representatives, particularly from the United States, are undertaking to influence the legislative process are proof that the reform of data protection law will also have repercussions well beyond the EU's borders.

The Conference of the Data Protection Commissioners of the Federation and of the *Länder* (federal states) also took an in-depth look at the reform package and adopted two resolutions: one at its 83rd conference in Potsdam, in which it called for a high level of data protection across the whole of Europe, the other at its 84th conference in Frankfurt/Oder, in which it called for a constructive and swift reform of European data protection law (cf. box a and box b for no. 2.1). In June 2012 the data protection commissioners submitted wide-ranging joint comments on the package of reforms (cf. Annex 5).

It is not surprising that the reform of European data protection legislation has recently been at the top of the agendas of the European data protection bodies, especially of the 2012 Spring Conference of European Data Protection Commissioners and of the Article 29 Working Party, which comprises the EU Member States' data protection authorities. The latter recently issued two detailed statements (WP 191 and WP 199, available in English at: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm; cf. also no. 2.4.1).

Box a for no. 2.1

Resolution adopted at the 83rd Conference of the Data Protection Commissioners of the Federation and of the *Länder* in Potsdam on 21/22 March 2012 calling for a high level of data protection across the whole of Europe

The Conference of the Data Protection Commissioners of the Federation and of the *Länder* supports the European Commission's intent to modernize and harmonize data protection in the European Union.

The draft of the General Data Protection Regulation contains rules which could lead to the further development of European data protection law, including
– the principle of technical data protection,
– the concept of privacy-friendly default settings,
– the principle of data portability,
– the right to be forgotten,
– better transparency on account of the responsible agencies' information obligations, and
– tougher sanctions for privacy violations.

The applicability of European law to providers from third countries whose services are directed at European citizens should also be highlighted.

The Data Protection Commissioners of the Federation and of the *Länder* believe it is essential that the highest level of harmonization of data protection law be achieved across all Member States. The Conference had already taken the view during the consultation procedure that, given the established traditions and legal standards applicable in the Member States and the EU's restricted legislative competence in regard to domestic data processing procedures in the public sphere, this objective can most effectively be achieved by means of a Directive. However, now that a Proposal for a directly applicable Regulation has been put forward, this must at least give the Member States the possibility of introducing, in their national laws, more far-reaching rules on data processing in public administration in the sense of a European minimum level of data protection which safeguards citizens' fundamental rights and creates the scope for innovative further legal developments in line with their respective legal traditions. Only then can, for example, the principles of data protection established in the consistent past decisions of the Federal Constitutional Court (*Bundesverfassungsgericht* (BVerfG)) be preserved and evolved in Germany.

The Conference acknowledges that the mandatory position of data protection officer is to be introduced for the private sector in Europe. Experience gained in Germany of data protection officers in the private sector acting in an independent supervisory and advisory capacity in an enterprise has been extremely positive. The Conference thus regrets that the Commission only intends to obligate companies with at least 250

employees to appoint a data protection officer. This will jeopardize the evolved and successful culture of private sector data protection in Germany.

The Conference feels that further steps are necessary over and above the modernization measures proposed in the draft Regulation. These were, for instance, proposed in a key points paper on a modern data protection law on 18 March 2010:

– Strict regulation of profiling, in particular a prohibition of the profiling of minors,
– Effective protection of minors, in particular by raising the age limit in relation to the need to obtain consent,
– Promoting self-data protection,
– Lump-sum compensation in the event of privacy violations,
– Simple, flexible and practicable rules on technical and organizational data protection which in particular recognize and delineate the principles of confidentiality, integrity, availability, non-linkability, transparency and the ability to intervene,
– The right to be able to use digital services anonymously or under a pseudonym, and
– The duty in principle to erase user data once the usage procedure has been completed.

The rules on risk analysis, prior checks and certification need to be stated more precisely in the Regulation itself.

The Conference regards the numerous powers which are to be conferred on the European Commission in regard to the delegated acts to be particularly problematical and feels that they need to be reduced to the strictly necessary minimum. All the rules essential to the protection of fundamental rights must be set out in the Regulation itself or must be established in the laws of the Member States.

Furthermore, the Conference draws attention to the fact that the consistency mechanism proposed in the draft of the General Data Protection Regulation, which involves the supervisory authorities in a complex consultation procedure, would interfere with the independence of data protection supervision and lead to the bureaucratization of data protection. It must thus be framed in simpler and more practicable terms.

The independence of data protection supervisory authorities (DPSA) as guaranteed under Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty

on the Functioning of the European Union (TFEU) also applies vis-à-vis the European Commission. The powers the Proposal delegates to the Commission in regard to concrete measures to be taken by the supervisory authorities when implementing the Regulation would thus not be compatible with the independence of the DPSA.

The Conference has repeatedly drawn attention to the importance of a high and uniform level of data protection, including in regard to police and judicial cooperation in criminal matters in Europe. It regrets that in this respect the draft Directive lags behind the draft General Data Protection Regulation and the standard of data protection established in Germany on many individual issues, for example the principles of data processing (like the principle of necessity) and the rights of the data subject (in particular on the protection of the "core area of private life"). The Directive should here also require as high a minimum level of data protection as possible across the EU, taking proper account of the Member States' constitutional traditions.

The Conference will constructively and critically support the legislative procedure.

Box b for no. 2.1

Resolution adopted at the 84th Conference of the Data Protection Commissioners of the Federation and of the Länder in Frankfurt/Oder on 7/8 November 2012 calling for a constructive and swift reform of European data protection law

The Conference of the Data Protection Commissioners of the Federation and of the *Länder* supports the European Commission's intention to achieve a high level of harmonized data protection across Europe. The Conference previously expressed its support in a resolution adopted on 21/22 March 2012. In two wide-ranging statements of 11 June 2012 the data protection commissioners of the Federation and of the *Länder* evaluated numerous individual aspects of the reform of data protection law and made recommendations regarding the further legislative process.

In light of the current discussions in Germany and in the Council of the European Union as well as relevant statements made by the Federal Government in regard to the reform process, the Conference would like to emphasize the following points:

– In view of the exemptions requested for the private sector, the data protection commissioners of the Federation and of the *Länder* consider it to be essential that the General Data Protection Regulation retain the previous system of data protection law. It should only be possible to process personal data if there is a statutory basis for doing so or the data subject has consented. The Conference rejects the exemptions the private sector is requesting in this context. If the intention were only to regulate individual instances of especially high-risk data processing and not to introduce rules on “ordinary data processing”, this would lead to a massive restriction of data protection and would significantly curtail data subjects’ rights.

Each processing of seemingly “irrelevant” data can have serious consequences for an individual, as the Federal Constitutional Court explicitly clarified in 1983. This applies today more than ever, which is why the Conference rejects exempting apparently “irrelevant” data.

As regards those cases in which the General Data Protection Regulation permits data processing, the Commission’s Proposal for a reform already contains suggestions for drawing a distinction on the basis of the risk posed by the data processing. This should be further expanded where such a risk-based approach is appropriate.

– The Conference expresses is strong support for retaining the tried and tested concept of uniform data protection legislation applicable to both the public and the non-public sectors and, in particular in regard to data processing in the public sector, of retaining the possibility of Member States introducing a higher standard of protection through their national laws.

– It considers it appropriate to lay down qualified minimum requirements in regard to employee data protection in the General Data Protection Regulation itself and to make it clear that Member States may enact more far-reaching data protection rules but that they may not fall short of those minimum requirements.

– With a view to the Directive on police and judicial cooperation in criminal matters, the Conference re-affirms the significance of a high and uniform level of data protection in this field and thus the importance of adopting a corresponding rule.

The Conference of the Data Protection Commissioners of the Federation and of the *Länder* calls on the Federal Government to advocate a high level of harmonized data protection in line with these positions in the Council of the European Union.

Accompanying the reform of EU data protection law is placing an enormous additional burden on my staff, as on account of the breadth of the reform it affects nearly all the divisions in my authority. In order to ensure our work is as effective and coordinated as possible, I have set up an internal project group formed of collaborators from various divisions.

2.1.1 The General Data Protection Regulation

The General Data Protection Regulation forms the core of the reform of European data protection law. It incorporates the key building blocks for the modernization of data protection legislation, which is why it is the focus of consultations in the Council of the European Union and of the public debate.

I basically regard the approach the Commission has adopted in the General Data Protection Regulation in a very positive light, since it provides the opportunity to finally address the long-overdue modernization of data protection law, which essentially dates back to the 1980s. In this context it should be borne in mind that the Federal Government regarded the implementation of the Data Protection Directive 95/46/EC in 2001 only as an intermediate step on the road to a comprehensive modernization of data protection legislation. At the time, the BMI commissioned a report which was to look at the need for reform and the necessary steps (cf. 19th Report, no. 1.2). The report by A. Roßnagel, A. Pfitzmann and H. Garstka (which is available (in German only) at: http://www.datenschutz.bund.de) provided and provides substantial material for a technical and academic debate. However, it was of hardly any consequence for data protection policy because no legislative activities ensued. Over the past ten years a few – in some cases quite significant – details of German data protection law have been amended; nevertheless, data protection legislation has undergone no comprehensive modernization (as to the modernization of data protection law, cf. also 23rd Report, no. 1).

However, despite my approval of the European Commission's initiative, significant improvements still need to be made to numerous aspects of the proposals. The debate on the reform is currently focusing on the following issues.

Basic regulatory structure

The General Data Protection Regulation retains the tried and tested regulatory principles and structures of applicable data protection legislation. Accordingly, personal data may only be collected, processed and used if there is a legal basis for doing so or if the data subject has consented. I have always opposed calls from the political realm and the world of business to give up this principle as regards "irrelevant data processing". I have the backing of the 69th Conference of the Association of German Jurists in this, which recently rejected such calls (cf. Resolutions of the 69th Conference of the Association of German Jurists, Munich 2012, p. 32 et seqq., available (in German only) at: http://www.djt.de/fileadmin/downloads/69/121206_djt_69_beschluesse_web_rz.pdf).

Only regulating individual instances of especially high-risk processing of personal data and leaving "ordinary" data processing largely unregulated would massively restrict data protection and significantly curtail the rights of data subjects. Every processing of seemingly "irrelevant" data can have serious consequences for individuals, as the Federal Constitutional Court clarified already in 1983. This applies all the more in the age of the Internet and with a view to ubiquitous data processing.

I, too, feel that it is right to take the risk the data processing poses to data subjects' rights as the point of reference regarding the substantive, organizational and formal requirements for safeguarding data protection. To some extent the draft General Data Protection Regulation already adopts this approach, but it may be expanded further.

However, neither should the scope of application of data protection legislation be narrowed nor the basic requirements applicable to the processing of personal data be lowered nor the basic rights of data subjects be restricted.

The 84th Conference of the Data Protection Commissioners of the Federation and of the *Länder* made its opinion clear in a resolution in which it called for a constructive and swift reform of European data protection law (cf. box b for no. 2.1).

The same data protection rules for public authorities and businesses?

The General Data Protection Regulation basically applies the same data protection rules to businesses, societies and associations, the self-employed and tradespeople

on the one hand and to authorities and other public bodies (excluding the police and criminal prosecution authorities) on the other.

This approach has already been established in the existing Data Protection Directive 95/46/EC and in most EU Member States' data protection legislations. However, Germany by tradition has separate regulatory systems for the public and the non-public sectors. This is essentially due to constitutional requirements: While in the case of data processing by the state the citizen is regarded as a holder of fundamental rights and the state is obligated to observe those fundamental rights, in the case of data protection law in the private sector the interests of the various holders of fundamental rights need to be balanced.

However, these constitutional differences need necessarily not mean that different data protection regimes have to be introduced. The basic principles are the same in both spheres even though they can be derived from different aspects of constitutional law. And it is becoming increasingly difficult to separate the two areas since the state is becoming more and more active in the private law sphere and is increasingly relying on private individuals in the performance of its tasks.

Nonetheless, the Member States should be given some leeway when it comes to putting the requirements set out in the General Data Protection Regulation into concrete form in their national laws. It must, among other things, be guaranteed that they can determine which categories of data are to be processed in the fulfilment of which tasks for which purposes and to which other agencies they may be transferred. Sector-specific data protection legislation contains a large number of such rules. As the draft of the General Data Protection Regulation already provides, data processing by the state must be based on EU or a Member State's law. This must be emphasized even more clearly in the Regulation in order to create legal certainty for the Member States in this respect. However, the new EU legal framework will have to be used to re-examine the very numerous and not always consistent sector-specific data protection provisions in German law.

I feel that proposals which advocate entirely deleting rules on data processing by public authorities in the General Data Protection Regulation and putting them in a directive are unrealistic. In my view, the required leeway can also be created within the context of the Regulation, and it is not necessary to call the entire regulatory structure into question and thus to jeopardize the reform. Especially in view of the increasingly intensive Europe-wide sharing of data between public authorities, I am

happy with the harmonization of data protection the Regulation also envisages in regard to the public sector. It would significantly increase the standard of data protection in some Member States and thus ultimately also improve the protection given to German citizens' personal data.

Has the Commission been given too many powers, or who will put the General Data Protection Regulation into concrete terms?

The draft General Data Protection Regulation contains a large number of powers entitling the European Commission to enact delegated acts or implementing acts. This possibility was introduced by the Lisbon Treaty and aims to give the Commission the power to enact concrete provisions in the same way as a statutory ordinance under German law. However, they may not refer to essential elements, which must be directly established in the legal acts (Regulation or Directive) by means of a formal legislative procedure.

In line with the data protection commissioners of the *Länder* and the Article 29 Working Party I am of the opinion that the Commission has gone much too far here. Delegated acts, for example, are envisaged in cases in which essential elements are to be regulated although they should in fact be included in the Regulation itself. In other cases there is no need for Europe-wide harmonization, as a result of which there is also no need for delegated acts either. In many cases it can also be left to the data controllers themselves, the everyday work of the supervisory bodies or the planned European Data Protection Committee to put the provisions of the General Data Protection Regulation into concrete form.

The Article 29 Working Party undertook an individual assessment of the delegation of powers in its Working Paper no. 199 (cf. no. 2.1).

The "marketplace principle": Application of data protection law also to non-European businesses

So far, whether European data protection law is applicable is dependent on whether a business is headquartered in the EU or at least uses data processing means which are located in the EU. However, the Internet makes it possible that businesses which are neither headquartered in the EU nor operate the means to process data in the EU can approach users within the EU with their offerings and process their personal data. Thus far no EU data protection legislation applies to such businesses, for

example the operators of social networks or search engines without a responsible branch office in the EU. This interferes with data subjects' rights, makes it more difficult for those rights to be asserted and represents a clear competitive disadvantage for businesses headquartered in the EU.

That is why, according to the General Data Protection Regulation, businesses headquartered outside the EU also have to comply with European data protection law if their services and sales activities are directed at the European Single Market and they collect personal data as a result. Data protection authorities in the EU welcome this "targeting approach", since the same framework conditions then apply to each instance of data processing directed at citizens living in the EU regardless of where the business is headquartered.

New data protection instruments: The right to be forgotten and the right to data portability

The risks associated with electronic data processing call for innovative approaches. The right to be forgotten and the right to data portability aim to foster data subjects' sovereignty over their own data, although how these rights are to be framed still needs to be re-examined.

The right to be forgotten aims to put data subjects in a position where they can assert their rights not only against the originator of data which were made public. They should also be able to require third parties to delete all links to and reproductions of the published data. The originator of the publication is therefore obliged, within the bounds of what is reasonable, to inform all those third parties who process the published data about the data subject's request to erase the data.

By informing the third party the body which originally published the data has, however, fulfilled its obligation. More specifically, it does not need to ensure that third parties using data it published actually comply with the request to erase the data. As was previously the case, this is left up to the data subject. In case of doubt, therefore, data subjects will not be able to legally assert their rights to have their data erased. Even if the "right to be forgotten" in its current form does not in fact fulfil the high expectations the term is raising, it is at any rate better than the current legal situation: Data subjects do not need to address themselves to a multitude of unknown third parties, but can turn directly to those responsible for publishing their data with their wide-ranging request for erasure and those, in turn, must inform the second- and third-party users of the published data. The right to be forgotten theoretically also

covers hard-copy publications, although it is entirely unclear how such a right could even rudimentarily be asserted. It would thus be desirable for the Proposal to be adapted accordingly (cf. box a for no. 2.1.1).

The right to data portability enables data subjects to request a copy of their data in electronic form and to transfer personal information from one provider to another. One only need call to mind users of a social network who wish to transfer their profile to another network. Nevertheless, this right is not limited to web 2.0 services, but also applies to other areas, for example electronic banking or online mail order purchases. Since the electronic recording of our everyday activities is marching on apace, for instance in the form of Internet click streams and profiles movement, surf or purchase behaviour, the right to data portability addresses a basic problem in regard to the right of informational self-determination. Because of the comprehensive quantities of data being stored, companies today know more about data subjects' interests and behaviour than they themselves do. Thus the aim behind the right to electronic surrender and portability is to give data subjects back a part of their data sovereignty. That is why I support this approach. However, it should be examined even here to what extent the rules lead to a sensible outcome in each individual case. It should be borne in mind that data subjects should not only be given the initial data they provided, but also the evaluations carried out by the relevant body. Further discussions are necessary on whether this will, ultimately, always be appropriate (cf. box b for no. 2.1.1).

Restrictions on profiling

Consolidating and linking of personal data in order to create profiles poses an especial risk to personal rights. Profiles enable a person's personality, especially their behaviour, interests and habits, to be determined, analysed and predicted. Often this profiling is done without the data subject's knowledge. This contributes to a feeling that one is constantly being analysed. Individual data profiles are an essential feature of the "transparent citizen" or "transparent customer". Profiles have entered many areas of our everyday life, in the form of consumer profiles, movement profiles, user profiles and social profiles, for instance. Even though profiling was already occurring in the offline world, it is only in the online world that profiles are posing an enormous threat to the right of informational self-determination on account of the wide-ranging means to make data available and to link them and because technical gadgets have penetrated into large parts of our everyday life.

That is why I am pleased to see that Article 20 of the draft Regulation contains a separate provision on profiling. Nevertheless, this does not go far enough, since it only addresses the use to which data already collected are put and then introduces certain bans on processing that data. An effective rule on profiling should not address the use to which such data is put, but should address the stage at which the personality profiles are created. Also, the dangers associated with profiling cannot be attended to merely by introducing prohibitions. Rather, what is needed are technical approaches, such as effective and irreversible anonymization and encryption mechanisms which limit the threat to personal rights. Vice versa, profiling using pseudonyms could be privileged in conjunction with a simultaneous ban on establishing a direct link to a specific person. The German Telemedia Act (*Telemediengesetz*) contains concepts which could also be applied to a European rule.

Strengthening technical data protection

Information processing and thus also data protection are subject to enormous technological changes. That is why I hope that the reform of European data protection law will more firmly establish the principles of technical data protection.

The draft of the General Data Protection Regulation contains numerous positive suggestions for strengthening technical data protection at European level. Technical data protection is accorded much more space than in the existing Directive. The Commission has obviously recognized the need to do significantly more when it comes to get to legal terms in this area. However, I feel that there is still some room for improvement with respect to some points:

Up-to-date and forward-looking data protection comprises technical and organizational measures which take appropriate account of data protection and data security. This is one of the central demands in the key issues paper entitled “A Modern Data Protection Law for the 21st Century” published by the Conference of the Data Protection Commissioners of the Federation and of the *Länder* in 2010 (cf. 23rd Report, no. 1.2).

The draft Regulation contains various principles and standards which could promote broad-based technical data protection. Chapter IV in particular deals at length with these issues. They include

– the obligation to “privacy by design”, i.e. to take into account data protection requirements when designing a system,
– the call for “privacy by default”, i.e. for default settings in social networks, for instance, which comply with data protection requirements,
– the duty to comply with technical and organizational principles of IT security to protect personal data,
– the duty to carry out a mandatory data protection impact assessment, or
– the repeated reference to the need to implement technical and organizational measures.

Unfortunately, the various aspects of data security and technical requirements are spread across numerous provisions without the huge significance of technical data protection being made clear in a central place wtihin the Regulation. Such a “key technical provision” should ensure that the elementary protective purposes of data protection – availability, integrity, confidentiality, transparency, non-linkability and the ability to intervene – are included as the goals of technical and organizational measures into the data protection principles established in the General Data Protection Regulation. These objectives are already recognized as the basis for carrying out technical and organizational measures both at European level (cf. Article 29 Working Party WP 196 on cloud computing, no. 5.3) and at national level (cf. Conference of the Data Protection Commissioners of the Federation and of the *Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, 2010, Chapter 3, available (in German only) at: www.datenschutz.bund.de, 23rd Report, Annex 6).

The draft Regulation contains many welcome, technology-neutral suggestions, including the following two examples:

The principles of “privacy by design” and “privacy by default” set out in Article 23 of the draft Regulation take account of the principles of data avoidance and data economy, which German data protection legislation already covers, as a central idea and develop them further. The aim is to enable possible data protection problems to be detected when new technologies are being developed so as to be able to incorporate data protection in the overall concept from the very beginning; it is often very difficult, time-consuming and expensive to solve data protection problems inherent to a system once it is already up and running (if it is possible at all).

Privacy impact assessments (PIA) are a further building block for implementing IT processes which meet data protection requirements. These PIA will play an

increasingly important role not only on account of Article 33 of the draft of the General Data Protection Regulation, but also on account of the European Commission pushing ahead with developing PIA for RFID systems (cf. 23rd Report, no. 5.9, Article 29 Working Party WP 180) and for smart grid/smart metering systems (cf. no. 10.1). So far, however, the overwhelming majority of these requirements are voluntary and non-mandatory. I therefore welcome the fact that PIA are now to be made mandatory in certain cases. The results of a PIA should not only be transparent for producers and users, but also for data subjects. That is the only way it will be possible to understand what risks are associated with which data processing procedures. Along with a duty to document the results, it should also be obligatory to subject those results to regular monitoring.

In view of the increasing significance of anonymization and pseudonymization as a means of designing more privacy-friendly IT systems and IT processes and of protecting privacy when using Internet services, these mechanisms should be explicitly enshrined in a central place within the legal acts.

Europe-wide minimum standard of employee data protection

The European Commission also aims to achieve a high level of employee data protection across Europe. I welcome this step. As is the case in the national debate (cf. no. 13.1), however, employee data protection is accorded only little space in the General Data Protection Regulation. Wide-ranging improvements thus need to be made to sufficiently meet the huge challenges being faced in this area.

Under Article 82 of the General Data Protection Regulation the Member States are, for example, to be granted the powers to establish their own rules in the field of employee data protection (which is why the draft Regulation only contains few rules in this regard), though only “within the limits of this Regulation”.

This restriction raises a couple of questions, given that each specific provision under national law in itself represents a deviation from the requirements made in the Regulation. Thus, the reference to “the limits of this Regulation” can only sensibly be interpreted to mean that national law must correspond to the terminology and principles of the Regulation and that it may not, as a whole, deviate from the standard of protection set in the Regulation.

In order to actually set a qualified minimum standard and thus to create a veritable added value for data protection in employee–employer relationships, the elementary standards in regard to employee data protection should be set out in a particular rule in the Regulation. In view of the significance and sensitivity of employee data, a high standard of data protection should be guaranteed. However, one cannot overlook the fact that a complete, Europe-wide harmonization of the specific requirements for guaranteeing a high standard of employee data protection will be very difficult to enforce. Thus the European Commission some time ago abandoned a specific legal act on employee data protection, a project launched more than ten years ago, since its prospects of success were low.

That is why the text of the Regulation needs to explicitly clarify that the Regulation only sets minimum standards in regard to employee data protection and that the Member States will be left free to enact more far-reaching requirements in the interest of data protection so that the level of protection already achieved in the Member States is at any rate not reduced. This demand was already made in the statement issued by the Conference of the Data Protection Commissioners of the Federation and of the *Länder* of 11 June 2012 on the General Data Protection Regulation and was re-affirmed in the Resolution adopted at the 84th Conference on 7/8 November 2012 (cf. box b for no. 2.1).

It is pleasing to see that the General Data Protection Regulation rules out consent as providing the legal basis where there is a significant imbalance between the data subject and the data controller. The draft Regulation thus puts into concrete terms the same principle of voluntariness as the precondition for the effectiveness of consent to the processing of personal data which is already established in Directive 95/46/EC and in the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG).

If the Member States were to be left to regulate the processing of personal employee data by statutory means alone, this would have huge practical implications. No reference is made to collective agreements (works agreements, service agreements and collective wage agreements). It is unclear whether the draft Regulation can nevertheless be interpreted such that the Member States may delegate this power to the employers/works councils and to the parties to collective bargaining agreements. That is why the General Data Protection Regulation should make it clear that collective agreements are also explicitly regarded as the basis of authorization for data processing so that these rules can be used to guarantee the same level of data protection for employees.

It is problematic that, according to the draft Regulation, the European Commission is also to be given the powers to enact delegated acts in regard to employment data protection. The Commission is thus given powers similar to the Member States when it comes to putting the Regulation in concrete terms, which would create a confusing legal situation if national law and delegated acts were to contain contradictory provisions.

Data protection officers in the private and public sectors – A successful model of German data protection legislation goes European

The rule on data protection officers to be designated by public authorities and bodies set out in the draft Regulation is of a conflicting nature. I welcome the fact that Article 35 of the draft provides for the mandatory designation of data protection officers by enterprises and public authorities/bodies. From the European perspective, this is a step forward, since the existing Data Protection Directive provides for the designation of inhouse data protection officers only as an option available to the national legislature (as an alternative to the comprehensive duties to notify to the data protection supervisory authorities).

By introducing Europe-wide data protection officers in businesses and public agencies the existing duties to notify automatic data processing to the supervisory authorities are to be dropped. And rightly so, since they have often proved to impose extra administrative burdens without creating any added value in terms of data protection.

By getting rid of these duties the Commission is unmistakeably drawing on the German rule, according to which the duties to notify are kept a bare minimum.

Since, however, the new obligation is only to apply to enterprises employing 250 people or more, it falls far behind the tried and tested German rule. The German rule provides for the general obligation for federal public agencies to designate a data protection officer; non-public agencies are obligated to designate a data protection officer if they have at least 20 employees (if they process data manually) or at least 10 employees (if they process data by automated means).

While introducing data protection officers in both enterprises and public authorities is thus to be regarded as progress from the European perspective, the proposed rules fall short of what is necessary. Under the new EU rule, approximately 0.3 per cent of

German businesses would thus have to designate a data protection officer only. The inappropriate threshold of 250 employees also disregards high-risk data processing, provides the opportunity for the rule to be bypassed and could, in consequence, lead to data protection officers largely being abolished in the private sector.

The threshold of 250 employees is not only much too high. The number of employees in a company is also not a suitable point of reference, because the need for internal data protection supervision is not dependent on the size of the company but on the extent of the data processing and the potential risk. Companies whose data processing is subject to prior checking or which transmit personal data on a commercial basis, such as address brokers or credit enquiry agencies, are rightly obliged under German law to designate a data protection officer irrespective of their size.

Unfortunately, the General Data Protection Regulation also lacks important instruments for safeguarding the data protection officers' independence, including the data protection officers' duty of confidentiality and the right to refuse to testify in court, the prohibition of discrimination and, above all, protection against unfair dismissal. Also, there is a difference between data protection officers being directly subordinate to the management (as in the Federal Data Protection Act) and, as proposed, their merely having the right to contact the management directly.

I will continue to work towards these important aspects being incorporated into the reform of the European legal framework and the status of data protection officers being strengthened across Europe.

Self-regulation: A mechanism for improving data protection

The European Data Protection Directive of 1995 already provides for the introduction of self-regulating mechanisms to promote data protection. This requirement was implemented into German law in 2001. However, this important tool has since led a shadowy existence, at least in Germany (cf. no. 3.4).

The draft of the General Data Protection Regulation also contains the existing requirement under European law and thus still provides for the possibility of creating codes of conduct at national and European level.

The Commission's proposals are, however, quite general and need to be rendered more precisely. Self-regulation can only succeed if the following preconditions are met:

– Codes of conduct may concretize and supplement substantive provisions in certain sectors, but may neither replace these nor establish new data processing powers.
– There must be clear legal requirements as to what may be the subject of codes of conduct (regulated self-regulation).
– The procedure for approving codes of conduct must be clearly regulated. It must be undertaken by independent, trustworthy bodies.
– It must be possible to enforce codes of conduct; the rights of the supervisory authorities may not be curtailed.
– Codes of conduct must be advantageous to companies, otherwise they will not find acceptance. The main advantages are greater legal certainty and the fact that the supervisory authorities are bound by the codes of conduct which they themselves have approved.

Some of the preconditions are already met in the Commission's proposals; others need to be ameliorated. Promising suggestions are being discussed at government departmental level which could be brought to bear in negotiations in the Council.

European data protection law must be uniformly enforced across Europe

The globalization of data protection as a consequence of the increasingly cross-border processing of personal data, especially via the Internet, by companies as well as public authorities means that the data protection authorities must adopt a common approach. It is true that the existing Data Protection Directive 95/46/EC has led to the harmonization of key privacy principles within the EU. However, it has not led to a sufficient level of standardized application of the law in the day-to-day practice of the data protection supervisory authorities, which are still organized at national level.

The European Commission has addressed this aspect. The "one-stop shop" (Article 51 para. 2 of the draft Regulation) and the consistency mechanism (Article 58 et seqq. of the draft Regulation) it proposes aim to contribute to standardizing data protection practice in the EU in those cases in which the controller has branches in several Member States or in which people in several Member States are affected by the same processing procedures. I feel that this kind of stronger harmonization of data protection practice by means of more intense cooperation between the

supervisory authorities is necessary. Added value could be created by means of a cooperation procedure which – in contrast to the “one-stop shop” proposed by the European Commission – would not be understood as an EU-wide competence on the part of one data protection authority, but as this authority being the central coordinator in those cases in which several Member States are affected. In addition, the new European Data Protection Board introduced in the draft Regulation must be able to contribute to EU law being interpreted and applied mandatorily in contentious cases and in cases which are of fundamental importance for EU data protection.

Despite the need for a greater harmonization of supervisory practice, one should not lose sight of the independence of the data protection authorities guaranteed under Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the EU (TFEU). It is above all not compatible with this independence for the draft Regulation to provide for the European Commission to have the power to suspend individual measures taken by authorities and to enact implementing acts “for the proper application” of the Regulation in view of those cases which are discussed within the consistency mechanism. It must be left to the supervisory authorities to apply the law, if the principle of independence is not to be rendered entirely meaningless.

Box a for no. 2.1.1

“The right to be forgotten”

The situation is familiar to all of us: Many years ago you published personal data on the Internet which you would rather no longer be associated with. Or worse still: A third party has published inaccurate data on the Internet. On account of search engines these data can be found for evermore. The understandable wish thus arose for a legal right and the technical means to be created for these data simply to be eliminated. In essence, in the Internet age the right to be forgotten thus means guaranteeing the right for personal data to be erased. The radical solution – a “digital eraser” which deletes data published in the Internet wherever it is located – will not be available any time soon: Data can be reproduced and disseminated any number of times worldwide. That is why the draft of the General Data Protection Regulation limits itself to moderately extending the right to have personal data erased which already exists under applicable law: The data controllers, insofar as they are able to do so, should also be responsible for the deletion of personal data they have transmitted to third parties.

Box b for no. 2.1.1

“The right to data portability”

Nearly all of us will at some stage have switched social network, mobile platform or Internet services providers and wanted to transfer our data to the new provider or platform. No matter how simple the switch can be, transferring one’s data to the new provider or platform can be an arduous process. Either the data cannot even be extrapolated from the previous provider’s database or the data formats are that different that they cannot be transferred to the new provider’s system. The right to data portability aims to provide a solution to these problems. Private individuals are to obtain their data in a format which they can transfer to a new provider. As number portability has become a standard procedure when switching telephone providers, this feature is now to be transferred to web 2.0 services.

2.1.2 A painstaking business – The draft of a new Directive applicable to police and justice

Together with the draft of a General Data Protection Regulation the European Commission has put forward a Proposal for a Directive applicable to police and justice. The Proposal is a step in the right direction, but needs further improvements. It is crucial that the Directive clarifies that it only sets minimum standards for national legislature.

The draft of a Directive regarding data protection applicable to police and justice plus the General Data Protection Regulation put forward at the same time aim to completely overhaul all areas of data protection following the entry into force of the Lisbon Treaty. I have supported this objective since the very beginning.

The concrete Proposal for a Directive has, however, given rise to mixed feelings on my part. It was and is important to me that as high a standard of data protection as possible be guaranteed across the whole of the EU. This applies in particular to police and justice and in regard to all data processing by the police, regardless of whether it is cross-border or not. The applicable Framework Decision 2008/977/JHA (cf. 22nd Report, no. 13.3.1) draws this distinction and, given that it is limited to cross-border data processing, it is precisely not suited to realizing this key objective. That is why a reform of the European data protection law in regard to police and justice is still necessary and has my backing.

At the same time, I can see that there are some problematical elements in the Commission's draft. One key aspect is the uncertainty regarding the level harmonization to be achieved by means of the Directive. In its decisions over the past 30 years the Federal Constitutional Court has ensured that a high level of data protection is guaranteed in Germany when it comes to the police in particular. I would like to call to mind its decisions in regard to the protection of the "core area of private life" (*Kernbereich privater Lebensgestaltung*), data retention, computer-aided profiling, or the obligation to label data collected by means of telecommunications surveillance. The Commission's Proposal lacks corresponding provisions. What would happen to these fundamental rules enshrined in German data protection legislation once the Directive entered into force? It is clear to me that anyone who decides to abdicate sovereignty to the European Union cannot expect things to always go their way according to one's own ideas. In contrast to data processing for commercial purposes, however, I feel there is no need to "put a lid on" domestic law and thus to risk legal disputes on a regular basis. That is why the Directive should make it clear that Member States can provide for a higher level of data protection in their national legislation than is provided for in the Directive. This would lay down a robust minimum level of data protection across the whole of the European Union. At the same time no Member State would be barred from creating new, more progressive data protection legislation. And the Federal Constitutional Court would continue to play an important role in developing the case law on data protection law together with the European Court of Justice.

I will continue to advocate improvements being made to the draft Directive. The principles applicable to data processing by police and justice should be aligned to the General Data Protection Regulation. Limitations on national processing should be passed on, citizens without any previous convictions better protected against being registered by the police, the possibility of transmitting data to unsafe third countries should be restricted and efficient data protection supervision ensured. This list includes only some of the tasks those involved in the proposed legislation will have to tackle.

The fate of the draft Directive is unclear. The Council in particular has adopted a very critical stance. I will advocate strengthening data protection as a whole in Europe without at the same time weakening individual Member States' existing legal safeguards. Introducing Europe-wide minimum standards in this area, which most especially affects fundamental rights, can pave the way towards doing just that.

2.2 More scope for security?

Cross-border cooperation between security authorities was further stepped up in the period under review. New legal instruments and the modernization of the technical means for the cross-border exchange of data both serve this purpose. I am critical of the fact that sensitive personal data are even transmitted to third countries without sufficient legal and actual guarantees.

2.2.1 European Investigation Order

A Directive regarding the European Investigation Order in criminal matters aims to facilitate cross-border criminal prosecution. Data subjects' fundamental rights must not be cancelled out as a result.

The European Investigation Order (EIO) leads to a wide-ranging recognition of decisions on investigation measures between the Member States. A Member State has to enforce the decisions of the investigating authorities and courts of another Member State. The draft thus distinguishes between the "ordering state" and the "executing state". In my opinion the draft Directive goes too far. It lacks rules on the applicability of sufficient minimum standards which adequately safeguard the fundamental rights of data subjects, including the right to data protection. The Conference of the Data Protection Commissioners of the Federation and of the *Länder* has also called for fundamental rights to be subjected to a high standard of protection (cf. box for no. 2.2.1).

The Treaty of Lisbon (cf. 23rd Report, no. 13.1) extended the possibilities for influencing criminal law and procedure at European level. On the one hand the Treaty makes it possible for the European legislature to set minimum standards here. On the other hand it can regulate the mutual recognition of Member States' decisions. The authors of the draft on the EIO rely on the latter possibility.

Mutual recognition and minimum standards are, however, interdependent. In other words, mutual recognition can only be expanded after comprising minimum standards have been introduced.

However, minimum standards in criminal proceedings are lacking in many areas. In particular, the Member States lack explicit rules in regard to the transfer, storage and use of data transferred. They should have regulated under which conditions

authorities can collect and use which data and for how long these may be stored. The use of those data should, in some cases, be restricted, for example in the case of data originating from investigation measures involving particularly intrusive interference (e.g. telecommunications surveillance, acoustic surveillance of the home). Data subjects' rights were to be laid down (hearing, information, notification, erasure, correction). The Proposal for a Data Protection Directive regarding police and justice likewise does not contain adequate rules on restricting the use of the collected data (cf. no. 2.1.2).

According to the Federal Ministry of Justice (*Bundesministerium der Justiz*, BMJ), the Proposal for a Directive at any rate also provides for the executing state to be able to examine the measure in accordance with its own laws. A German authority could thus examine whether a measure would, for example, violate the Code of Criminal Procedure (*Strafprozessordnung*, StPO). If so, that would constitute a reason to refuse enforcement of the measure.

However, the grounds for refusing enforcement of a measure are insufficient in some key areas, for example when it comes to transferring personal data between Member States. According to the Proposal, the authority in the executing state is to be under very wide-ranging obligations to transmit data from its own databases and to make available any evidence at hand. If the Code of Criminal Procedure restricts access, for example because personal data from telecommunications surveillance can only be used in the case of criminal acts of a special weight, according to the Proposal this restriction will likely be dropped. At any rate – and contrary to the German Code of Criminal Procedure – the Proposal does not contain a corresponding rule. The wide-ranging obligation to enforce EIOs "by non-coercive means" is vague.

The Proposal for a Directive regarding the EIO has not yet been adopted; negotiations are still ongoing at political level. I recognize that the Federal Government is endeavouring to safeguard rule-of-law standards by, as far as possible, ensuring that domestic law acts as the barrier to inter-state transfers of data. Nevertheless, I would like to see clearer minimum standards at European level, since citizens across Europe should be able to trust in the legislature taking account of their fundamental rights in Directives and Regulations and shaping these accordingly. The draft of an EU Directive on data protection applicable to police and justice currently under discussion provides an opportunity to move closer to reaching a satisfactory solution (cf. no. 2.1.1).

Box for no. 2.2.1

Resolution adopted at the 83rd Conference of the Data Protection Commissioners of the Federation and of the *Länder* in Potsdam on 21/22 March 2012 calling for the European Investigation Order not to cancel out fundamental rights guarantees

Consultations are currently ongoing at European level on the draft of a Directive regarding the European Investigation Order in criminal matters, which has huge implications for the protection of citizens' fundamental rights in the EU Member States. It could lead to the constitutionally guaranteed standard of protection in regard to criminal procedural measures sinking to the lowest common denominator across Europe. It could, for instance, lead to a Member State collecting data or evidence for another Member State and transmitting them although the collection would not be permissible under its own laws.

The Proposal for a Directive pursues the primary objective of permitting the extensive mutual recognition of criminal prosecution authorities' decisions to take interfering measures without uniform procedural guarantees having been established. This raises problems where lower standards of protection apply in the ordering state than in the executing state. Member States do not always have adequate possibilities for rejecting an order issued by another Member State. Intervention thresholds, rules on purpose limitation and procedural rules must guarantee that the data subjects' personal rights are observed.

Effective, cross-border prosecution in a united Europe must not go to the detriment of the protection of data subjects' fundamental rights. The requirements set out in the EU Charter of Fundamental Rights must be consistently applied. The European Investigation Order must be embedded within a logical overall concept for data collection and use in the field of internal security and prosecution which guarantees citizens' fundamental rights.

2.2.2 Europol analysis work files

The processing of personal data in analysis workfiles at the European Police Office was controlled according to data protection law.

I have in previous Reports repeatedly addressed the tasks and working methods of the European Police Office (Europol) (cf. most recently in the 23rd Report, no. 13.11).

In 2012 the Europol Joint Supervisory Body (JSB) put a priority on the inspection of files which Europol established for its analysis purposes. Its Inspection Report was not yet available to the public as this Report was going to press. Inspection Reports – insofar as public versions are made available – can be downloaded from the JSB's website (http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en). Nevertheless, several things can be said about the operation of the analysis work files and about the data protection problems involved.

Analysis work files are established for a limited period of time for specific phenomena and offences (e.g. fighting organized crime or terrorism). By means of them Europol is processing personal data originating from the Europol member states and third countries. The aim is for new findings and traces as to investigations – including for authorities in the member states.

Council Decision 2009/936/JHA of 30 November 2009, which was published on 11 December 2009 in the Official Journal of the European Union (OJ L 325 p. 14 et seqq.), establishes which data may be processed under which conditions in the Europol analysis work file. Accordingly not only data on suspects, but also on contacts and associates, witnesses, victims, and informers and whistleblowers, may be processed. Correctly assigning a data subject to these categories of persons is of decisive importance.

According to the aforementioned Decision, contacts and associates are those persons through whom there is sufficient reason to believe that information can be gained concerning (potential) offenders or suspects which is relevant for the analysis. Thus a "contact" is anyone who has sporadic contact with one of these people – regardless of why. Someone having regular contact is defined as an "associate" according to the Decision.

Very far-reaching – even strictly personal – data on contacts and associates within this meaning may be stored, insofar as there is reason to believe that these data are necessary for analysing the data subject's role as a contact or associate. This is sufficient to be able to process information on a contact or associate, as for instance

– on their economic and financial situation (cash assets, share holdings, bank and credit contacts, other information revealing their management of their financial affairs etc.),
– on their behaviour (lifestyle, habits, places frequented etc.),
– from other databases in which information on the person is stored (e.g. public and private entities),
– on legal persons in context with certain information.

I was already critical of this before the Council adopted its Decision. According to the Federal Constitutional Court, the German police may collect and process data on contacts and associates only under much stricter conditions. “The precondition is concrete facts establishing an objective link to the act and thus involvement in the commission of the criminal act as a whole, in particular involvement in the background or the surroundings of the offences” (Federal Constitutional Court, case file 1 BvR 1104/92 of 25 April 2001). In establishing the criterion “concrete facts” the Court has already set a considerably higher threshold than the Council Decision does, which merely requires its necessity or sufficient grounds.

The standards of the Federal Constitutional Court are binding in Germany; the police must comply with them.

2.2.3 CIS – An information system not needed

The Joint Supervisory Authority on Customs found that the customs authorities in the Member States hardly ever enter any data into the Customs Information System – and suggests abolishing it.

The Customs Information System (CIS) is overshadowed by more well-known European information systems, such as the Schengen Information System (SIS) and the Europol Information System (EIS, cf. no. 7.6.2). The CIS is a technically and legally complex construct which serves various purposes. It is intended to support European customs authorities in preventing and prosecuting serious violations against the customs legislation of individual Member States and against EU customs law.

The customs authorities of the EU Member States hardly use the CIS or even do not make use of it at all; only very few data have been entered into the system by the customs authorities. This was the conclusion drawn following an inspection carried

out by the Joint Supervisory Authority of Customs in the European Anti-Fraud Office (OLAF, the agency responsible for the technical operation of the database) and which my authority was involved in. I had already myself established that this was the case during the 2005/2006 reporting period (cf. 21st Report, no. 32.5) when I made enquires with the Customs Criminal Investigation Office (*Zollkriminalamt* (ZKA)) about the CIS. Obviously nothing has changed in regard to the lack of acceptance by the EU Member States' customs authorities.

That is why it is only logical for the Joint Supervisory Authority of Customs to suggest, based on its inspections, that the CIS be abolished since there is obviously no need for it.

The Member States have, unfortunately, not yet reacted to this recommendation. It is obviously easier for those responsible to decide to set up new files, databases and information systems than to abolish them once they have proven useless. This costly asymmetry could perhaps be avoided if the need for such systems was not only asserted but also substantiated before they are set up.

2.2.4 Eurodac

In future the Eurodac database of fingerprints is said to be even made available to prosecuting authorities. From the data protection point of view this is to be criticized.

The European Commission's proposed amendment of the Eurodac Regulation of September 2012 aims to give the criminal prosecution authorities access to Eurodac data under certain conditions. In a joint letter to the European Commission the Eurodac Supervision Coordination Group and the Article 29 Working Party of the Data Protection Commissioners of the Member States of the European Union emphasized that the European Commission did not provide evidence of why the instruments currently available to the prosecuting authorities were not sufficient and why access to data on asylum-seekers was necessary. Against this backdrop the two groups of data protection commissioners do not feel that it is justified to change the purpose limitation of the data stored in Eurodac. As this Report was going to press negotiations in the European Council and in the European Parliament regarding the European Commission's proposal had not been concluded.

The Eurodac Supervision Coordination Group looked into two coordinated inspections. It first examined the provisions Member States had undertaken in order

to implement the duty to erase fingerprint data ahead of time – for instance when an asylum-seeker acquires the nationality of a Member State before the end of the retention period (of up to 10 years). My inspection showed that the Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge*, BAMF), the central body responsible for the national part of the Eurodac system, had ensured the relevant exchange of information with the naturalization authorities. Shortcomings as regards the flow of information were, however, found in some Member States. The Secretariat of the Eurodac Supervision Coordination Group affiliated to the European Data Protection Supervisor (EDPS) published the inspection report (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/11-12-09_EURODAC_Report_EN.pdf). The second inspection looked into the processing of illegible fingerprints and was nearing completion as this Report was going to press; however, a report was not yet available.

2.2.5 Visa Information System

The European Visa Information System (VIS) is fully operational.

After many years of planning and preparation, the European Visa Information System (VIS), a new multinational database, was taken into operation on 1 October 2011 (cf. no. 8.9). The VIS serves similar purposes as Eurodac (incl. avoiding multiple applications, identity verification, cf. no. 2.2.4), but covers a different group of people. The VIS database not only collates personal data on visa applicants and stores these for up to five years, it also includes personal data on those who issue invitations to visit to applicants who need a visa. Next to standard information such as family name, first name and date of birth, visa applicants' biometric data (photographs and fingerprints) are also stored.

Unlike in the case of Eurodac, data for the VIS are not usually collected by domestic authorities, but by the Member States' consulates and embassies abroad and then passed on to the central VIS database in Strasbourg via national units. The VIS is currently being used in the foreign representations of participating states in North Africa, the Middle East and the greater Persian Gulf region (cf. box for no. 2.2.5). The European Commission is set to take a decision on whether to include further regions and countries.

Data protection supervision in regard to the VIS is based on a similar model to Eurodac: The EDPS supervises the central VIS database whilst the data protection authorities of the Member States oversee the respective national components of the

VIS. I am responsible for data protection supervision in Germany since the Federal Foreign Office (*Auswärtiges Amt*, AA) and the Federal Office of Administration (*Bundesverwaltungsamt*, BVA) are responsible for the national component of the VIS. In order to coordinate the work and the focus of supervision in the Member States a joint supervisory body chaired by the EDPS was also created for the VIS; I am also a member of that body.

Box for no. 2.2.5

Regions in which the European Visa Information System operates (as at: end of 2012)

Region 1: Northern Africa

– Algeria
– Egypt
– Libya
– Mauretania
– Morocco
– Tunisia

Region 2: Middle East

– Israel
– Jordan
– Lebanon
– Syria

Region 3: Greater Persian Gulf region

– Afghanistan
– Bahrain
– Iran
– Iraq
– Kuwait
– Oman
– Qatar
– Saudi Arabia
– United Arab Emirates

– Yemen

2.3 IT goes Europe

Increasingly, decisions regarding the processing of personal data by public agencies are no longer being taken at national level alone. Not only the legal framework but technical standards are also being set by the European Union. In addition, the EU and the agencies it is establishing are more and more themselves operating large-scale Europe-wide systems as well. Unfortunately, the Commission's proposals for a new legal framework for data protection in the EU (cf. no 2.1) ignores EU institutions and the IT systems operated by them. The same applies to their data protection supervision structures.

Separate supervision bodies, known as Joint Supervisory Bodies (JSB), have been set up for various information systems operated by European agencies (Schengen Information System, Europol, Eurojust, Customs Information System).

In contrast, the EDPS and the national supervisory bodies cooperate closely both when it comes to supervising the European fingerprinting system (Eurodac, cf. no 2.2.4) and the newly established Visa Information System (VIS, cf. no. 2.2.5). On 1 December 2012 the EU Agency for large-scale IT systems, which was established in November 2011, took over the operational management of the central databases of Eurodac and of VIS. In addition, the Agency is also to be responsible for managing the second-generation of the Schengen Information System (SIS II), probably as of spring 2013.

I advocate standardizing the various models for monitoring and supervising European IT systems in regard to data protection law. As well as creating synergy effects this could make data protection supervision more effective by introducing a uniformly high standard for all EU citizens.

2.3.1 Internal Market Information System

The IMI Regulation entered into force in December 2012. It permits information sharing and communication between the EU Member States on the basis of the Directive (EC) on services in the internal market.

The Internal Market Information System (IMI) went live in early 2010. It enables numerous authorities in the 27 EU Member States to communicate electronically, for instance where there are doubts as to the authenticity of documents submitted by a

service provider and inquiries thus need to be made with the competent authority in the issuing Member State (cf. 22nd Report, no. 3.4.1).

The IMI Regulation ((EU) No. 1024/2012) entered into force in December 2012 and established the legal framework which had been lacking up until then. The Regulation creates legal certainty when it comes to dealing with personal data in the IMI and is a key precondition for the mandatory application of data protection principles when using the IMI.

I was informed by the Federal Ministry of Economics and Technology (*Bundesministerium für Wirtschaft und Technologie*, BMWi) about negotiations on the draft IMI Regulation and was given the opportunity to submit my own comments. Even though I was unable to assert all of my positions, the competent Council working group did manage to achieve viable compromises.

I will continue to keep an eye on the IMI Regulation and will – together with the data protection commissioners of the *Länder* – ensure compliance with the provisions on data protection. The IMI Regulation provides for independent supervision as regards the lawfulness of processing of personal data by IMI actors in their Member State and it provides for guaranteeing the protection of data subjects' rights by the national data protection authorities. Furthermore, also the EDPS can, where necessary, invite the national supervisory authorities to meetings in order to guarantee supervision of IMI and its use by the IMI actors.

2.3.2 epSOS: How to protect health data when transferred cross-border?

The Article 29 Working Party has issued data protection recommendations regarding the implementation of a European pilot project on the cross-border transfer of health data.

Health data not only provide information about a person's state of health, medications and necessary treatments, they also enable wide-ranging predictions to be made about how that person's health will develop in the future; and they are of great economic value. That is why they are of great interest to diverse stakeholders in business, health system and public administration. They are subject to medical confidentiality and – if they are used by social benefit agencies for tasks set out in the Social Code (*Sozialgesetzbuch*, SGB) – to the special protection of the Social Code.

The Federal Data Protection Act and the European data protection law also classify such information as especially sensitive data.

Health data also play a role in the international context. epSOS (Smart Open Services for European Patients – Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription) is an EU-funded project in the context of which European citizens are to be offered cross-border e-health services. The main emphasis is to be on developing a Europe-wide infrastructure for providing access to health-related data across national borders so as to improve health services for patients who are staying in another EU country.

Key examples of cases in which the epSOS infrastructure will be used include cross-border access to an electronic patient summary and an electronic prescription (e-prescription). The patient summary will be stored in the patient's Member State and will contain information on illnesses, relevant operations and intolerances, similar to an electronic patient file. The aim of the e-prescription is to enable prescriptions to be issued when a patient is being treated in another European country. To that end the pharmacist or physician at the place where the patient is staying will be able to access the medications file (which is part of the patient summary) in the other Member State. The health data will only be transferred with the data subject's consent.

Even though Germany is not yet involved in the project, which is still in its test phase, I was involved in the drafting of data protection recommendations for epSOS by the the Article 29 Working Party's Health Data Subgroup (available at: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm). According to these recommendations the data subject's explicit consent is required in regard to participation in the project, the provision of medical data and the concrete data transfer. It is just as important that a high standard of technical security apply to the transfer of the data, for example by end-to-end encryption.

The high standard of data protection which applies to the German electronic health card must continue to be guaranteed, including the cases of cross-border data processing. This aspect is of especial importance to me and something I will continue to work towards.

2.3.3 Social data no longer know any borders

For the electronic exchange of social data at European level (EESSI) the legal basis has now been created.

The free movement of workers is one of the fundamental freedoms established in the EU. If insured employees have worked in several Member States, information on them and members of their family is entered into the social systems of several Member States. The social security authorities need to exchange a lot of this information. In particular the social security authorities in the country of origin are dependent on receiving this information from the social security authorities of those states in which the work was performed. So far a number of different hard copy forms have been used to exchange these data. Drawing up the relevant forms in the respective national languages is time-consuming and expensive. Sometimes applications are rejected on account of their being incomplete, incorrect and illegible.

In future, the cross-border flow of social insurance information is to be handled electronically. The more than 15 million notifications sent annually by national authorities are in future to be transmitted via the EU-wide Electronic Exchange of Social Security Information (EESSI) IT system. The EESSI will be incorporated into the EU's administrative network sTESTA. The Member States will be responsible for establishing their own national infrastructures. A register of national institutions in the healthcare, pensions, unemployment and family benefits sectors, which are to be included in the electronic exchange of data, is available online at: http://ec.europa.eu.

The EU has adopted rules in the form of Regulations to establish the EESSI (Regulation (EC) no. 883/2004; Regulation (EC) no. 987/2009). They are directly applicable in the Member States and neither clarify questions regarding domestic competence nor do they meet the requirements of data protection. Relevant additional provisions which put the rules into concrete form were therefore adopted in Germany in the Act on the coordination of social security systems in Europe (*Gesetz zur Koordinierung der Systeme der sozialen Sicherheit in Europa*) of 22 June 2011 (Federal Law Gazette I 2011 p. 1202).

During the legislative process I paid very particular attention to ensuring that the agencies coordinating the flow of data between the Member States are only given the powers they actually need in the performance of their tasks. The aforementioned Act also clarifies how the social insurance carriers (e.g. health, pension and accidence

insurance companies) in the country of origin are notified when an insured person is posted to another Member State.

Further, the Act determines liaison offices and access points in Germany. The liaison offices are responsible for answering enquiries and requests for mutual assistance from partner states. The access points act as national contact offices for the electronic data exchange and for passing on documents and other information at national level. In Germany five such access points are being set up with large social insurance carriers.

The legislature took up my suggestion that the use of all data, i.e. including occupational benefit systems, family benefits (child benefit, parental allowance etc.) and provisions for civil servants, are to be subjected to the strict privacy rules applicable according to the Social Code.

The IT systems necessary for safeguarding the safe transfer of data in line with the relevant provisions are not yet available. In view of the numerous participating states and the various legal and technical conditions which need to be fulfilled, this is still proving difficult. I will review the technical implementation in due course in order to examine whether it conforms to data protection law. The EESSI should be fully operational from May 2014 – time is thus running short when it comes to standardizing and implementing the necessary protective measures in line with data protection legislation.

2.3.4 Europe-wide electronic identification only if data protection is not compromised!

Considerable amendments regarding privacy issues still need to be made to the planned EU Regulation for the mutual recognition of electronic identification within the European Union.

On 7 June 2012 the European Commission put forward a Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market. Its objective is the Europe-wide mutual recognition of electronic identification systems and the harmonization of rules on electronic trust services, such as electronic signatures and delivery services.

The eID function on the new personal ID card can currently be used in Germany for electronic identification purposes. Citizens can, for instance, use the function to prove their identity to a local authority. The local authority electronically accesses the data on the ID card which they need to unequivocally identify the person in question. The eID function can also be used when making online purchases. It is to be ensured that access to personal data on the ID card is restricted to that information which is absolutely essential for the application in question. For example, where someone wishes to pay to download age-restricted videos, the seller needs to know the customer's age, but no more. The seller does not, in such cases, need to know the customer's name.

This data protection-friendly function, which makes it possible to use a pseudonym, is called into question in the Proposal for a Regulation, because the Proposal requires the identifying data to be clearly attributable to the natural or legal person. In addition, mutual recognition has only been regulated in principle. Unequivocal and concrete rules on data protection and data security are lacking, for example. The high level of data protection achieved on account of the German eID function cannot be allowed to be diminished on account of the obligation to recognize other Member States' electronic identification systems if they do not even remotely meet the standard of data protection established in Germany. That is why I welcome the fact that the Federal Government is committed to establishing rules on electronic identification at European level which meet data protection requirements.

2.4 European and international cooperation on data protection

Active data protection encompasses cross-border cooperation between data protection authorities. A lot has happened in this matter in the period under review.

2.4.1 The Article 29 Working Party

2.4.1.1 The Future of Privacy subgroup

The Future of Privacy subgroup is responsible for fundamental aspects of data protection at EU level. In the period under review it focused on the European Commission's Proposal for a General Data Protection Regulation (cf. no. 2.1.1) and prepared two opinions issued by the Article 29 Working Party.

In its Opinion 1/2012 (WP 191) adopted on 23 March 2012 the Article 29 Working Party is welcoming the Commission Proposal with a view to strengthening the position of data subjects, extending the obligations of data controllers and improving the status of supervisory bodies at national and international level. Despite its basically positive attitude to the Regulation, the Data Protection Working Party is of the opinion that some aspects of the Proposal need refining and improving. In its Opinion 8/2012 (WP 199) adopted on 5 October 2012 the Article 29 Working Party provided further basic input on the Commission's Proposal for a General Data Protection Regulation. The Opinion includes, among others, a review of all powers to be delegated to the European Commission according to the Proposal.

In addition, the subgroup looked at the protection of special categories of personal data, notification obligations and practical cooperation between data protection authorities. The results of its consultations were summarized in so-called Advice Papers which were sent to the European Commission as the Article 29 Working Party's contribution to the reform debate.

A list of opinions and other documents adopted by the Article 29 Working Party in the period under review is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

2.4.1.2 International Transfers subgroup

The International Transfers subgroup focused on binding corporate rules (BCR) for the transfer of personal data to third countries, especially for processors.

The International Transfers subgroup dealt with a number of issues related to the transfer of personal data to third countries. According to Article 25 para. 1 of the European Data Protection Directive 95/46/EC, such transfer is only permissible where an appropriate level of data protection is guaranteed in the recipient state, a requirement which is often not met.

In order nevertheless to enable data transfers within globally active groups of companies, BCR are being developed on the basis of Article 26 para. 2 of the Data Protection Directive. In view of the increasing cross-border data streams, these are gaining in importance. The European procedure for the mutual recognition of BCR (cf. 23rd Report, no. 10.1) is now successfully being applied in practice. Some 40

such BCR have since been adopted Europe-wide; some 20 are currently at the coordination stage.

In the period under review the subgroup also developed BCR for processors, for which there is felt to be a great need on account of technical developments, particularly as regards cloud computing. The Article 29 Working Party's Working Paper (WP) 195 adopted on 6 June 2012 lists, in tabular form, the required building blocks for such BCR for processors. A respective application form was adopted as well. The documents are available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. The EU-wide procedure for the coordination and recognition of BCR for data processors will be available to businesses from 1 January 2013.

The countries participating in the Asia–Pacific Economic Cooperation (APEC) use a procedure similar to the European BCR system for international data transfers (called cross-border privacy rules (CBPR)). A working group comprising representatives of the APEC and members of the International Transfers subgroup, which I am also involved in, is attempting to harmonize the two systems and, if possible, to establish a certain degree of interoperability between BCR and CBPR. The goal is to make it easier for globally operating companies to transfer personal data across borders within their group of companies and at the same time to guarantee a global level of data protection as homogenous and as high as possible.

2.4.1.3 Technological data protection also in Brussels – Chair of the Technology subgroup

A representative of the Federal Commissioner for Data Protection and Freedom of Information took over the chair of the Technology subgroup in October 2010. The subgroup deals with technological data protection issues and is the largest of the Article 29 Working Party's subgroups, with more than 30 members.

In October 2010 a member of my agency assumed the chair of the Technology subgroup in Brussels. According to the Article 29 Working Party's work programme, this subgroup focuses on technological challenges facing data protection.

Over the past two years the Technology subgroup has drafted various opinions on behalf of the Article 20 Working Party. They include working papers on facial

recognition, notification of data breaches, RFID PIA (cf. 23rd Report, no. 5.9), behaviour-based Internet advertising and smart metering (cf. no. 10.1).

One of the most wide-ranging and most important opinions – for which representatives of the *Land* data protection commissioners and my agency acted as rapporteurs – is the paper on cloud computing (cf. no. 5.3). It describes the dangers and risks of data storing and data processing "in the "cloud", analyses the applicable law and the obligations incumbent upon data controllers, and contains recommendations for cloud users – also in the context of data transfers to third countries.

In addition, the subgroup drafted opinions on current issues which are of relevance to technical data protection. One main emphasis over the past two years was placed on the assessment of Google's new Privacy Policy (cf. no. 5.9). Another important issue covered the data protection rules and the practice of the social network Facebook (cf. no. 5.8.1).

2.4.1.4 The new "B(ee)TLE"

As a consequence of the changes brought about by the Lisbon Treaty the Article 29 Working Party set up the new BTLE (Borders, Travel & Law Enforcement) subgroup.

The new subgroup deals with data protection issues in the fields of border and migration control and police and judicial cooperation in criminal matters. The most prominent issues so far were the transfers of airline passenger data and of payment transaction data to the United States.

By means of the Lisbon Treaty the special role previously accorded police and judicial cooperation in criminal matters (cf. 23rd Report, no. 13.5) has largely been abandoned. The Article 29 Working Party reacted to this basic development by setting up the new Borders, Travel & Law Enforcement (BTLE) subgroup in summer 2011. The new subgroup takes up the previous work of the Article 29 Working Party, which already had been intensely occupied with the transfer of airline passenger data for police purposes prior to the signing of the Lisbon Treaty.

At the same time the European data protection authorities are pooling their advisory competences within the BTLE subgroup as regards the central data protection issues in the field of police and justice. The 2012 Spring Conference of European Data

Protection Commissioners therefore agreed to disband the Working Party on Police and Justice which had previously dealt with these issues.

Since it was established, the BTLE subgroup has drawn up a number of contributions and opinions on privacy issues. The elaboration of an opinion on the draft of a new Directive applicable to police and justice (cf. no. 2.1.2) occupied a lot of its time. Further, the subgroup prepared several statements issued by the Article 29 Working Party on various initiatives and treaties which serve the increased use of airline passenger data for police purposes within and outside of Europe (cf. no. 2.5.2). In addition, the treaty on the transfer of payment transaction data concluded with the United States and the European Commission's ideas in regard to creating a comparable European programme (cf. 2.5.1) were of great importance in regard to data protection policy. In a letter to the European Commission prepared by the BTLE subgroup, the Article 29 Working Party commented on the Commission's Communication on "intelligent borders" (cf. no. 2.5.3.3).

It is already clear by now that much remains to be done in all these areas. The same goes for a new large-scale project in the airline industry which will no doubt cause a great stir, that is the Checkpoint of the Future (cf. no. 2.5.3). Both in regard to these and other projects the BTLE subgroup seeks a critical dialogue at experts' level with representatives from the European Commission and the industries involved.

The subgroup is coordinated by a member of my agency together with a Dutch colleague.

2.4.2 European Data Protection Conference

In the period under review the annual Spring Conference of European Data Protection Commissioners focused on the EU's reform of data protection law (cf. no. 2.1).

The 2011 Spring Conference, held in Brussels on 5 April, was jointly organized by the European Data Protection Supervisor and the Chair of the Article 29 Working Party. It adopted a Resolution which emphasizes the need for a comprehensive EU data protection legal framework covering even the areas of police and justice.

The text of the Resolution is available at:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/11-04-05_Spring_conference_Resolution_EN.pdf.

The key issue at the Conference organized by the National Commission for Data Protection (CNPD) in Luxembourg on 4 May 2012 was likewise the reform of EU data protection law. In its Resolution the Conference welcomes the core objectives of the reform project, namely to strengthen the rights of data subjects, to introduce the principle of accountability for data processing agencies and to strengthen the role of independent data protection authorities.

In addition, the Conference looked at possibilities for strengthening the rights of Internet users, especially in regard to cloud computing and social networks, the protection of personal data in the areas of police and justice, and the modernization of other international data protection regulations, in particular the Council of Europe's Data Protection Convention 108 and the OECD Guidelines (cf. no. 2.4.5).

The text of the Resolution is available on the CNPD's website at:
http://www.cnpd.public.lu/fr/actualites/national/2012/04/spring-conference-2012/Resolution_on_the_European_data_protection_reform.pdf.

Case handling workshops were held also in 2011 and 2012 under the auspices of the European Data Protection Conference; members of my agency took part in the workshops. These meetings have proved very useful for sharing experience and know-how at European level and thus for developing comparable methods of dealing with citizen's petitions and handling similar issues in a comparable manner. The last two workshops were held in Warsaw (in October 2011) and in Budapest (in September 2012). The main emphases included data protection in social networks, data protection in the workplace, and ways and means of dealing with cases and complaints involving the cross-border transfer of personal data. The target group of these case handling workshops primarily includes those members of staff in the data protection authorities who deal with concrete problems and issues (at working level). The individual workshops are open to members of data protection control agencies across the whole of Europe. That is why data protection authorities in states which are not (yet) members of the EU can benefit from the exchange of experiences.

2.4.3 International Conference of Data Protection and Privacy Commissioners

Also in the period under review the international conferences of data protection authorities from around the world provided many impulses for further stepping up cooperation in a globalized data world.

The 33rd International Conference of Data Protection and Privacy Commissioners, held in Mexico City in 2011, was hosted by the Mexican Federal Institute for Access to Public Information (IFAI). The title of the conference was “Privacy: The global age” and it dealt with issues concerning the internationality of data protection and data security. In view of increasing global data streams the extent of which each day exceeds new superlatives, the right to the protection of personal data can only be guaranteed effectively by means of coordinated action at international level. Several resolutions were adopted which aim to bring about more intensive cooperation between data protection commissioners, who travelled from all over the world to take part in the conference. The aims are to make possible data protection authorities’ access to the international conference by means of a clearly regulated accreditation procedure to develop a concept for deepening international cooperation between supervisory authorities and to improve cooperation between data protection authorities on enforcing data protection.

On my initiative the conference voted unanimously to adopt a Resolution on the Internet Protocol Version 6 (IPv6) with a view to the uniform use of identifiers when implementing the protocol (cf. also no. 5.6). Another resolution concerned standardized data protection in the event of a disaster, including simplifying the exchange of data based on data protection standards.

The 34th International Conference of Data Protection and Privacy Commissioners, which was held in Uruguay in 2012, was organized by the Personal Data Regulatory and Control Department of Uruguay (URCPD). The focus of the conference the motto of which was “Protection of Personality and Technology in Balance” laid on stepping up cooperation and information sharing between data protection authorities around the world, an issue which was also addressed in depth in a Resolution. The Resolution on cloud computing, which I had prepared and which was unanimously adopted by the conference, contains six basic recommendations regarding data processing “in the cloud” (cf. also no. 5.3).

Profiling formed another main technological focus at the conference. Conference attendees discussed developments regarding profiling on various continents both in the public and in the non-public sectors. They realized that the consolidation and linking of personal data to create profiles poses an increasing threat to the right of personality. The conference hosts addressed the problem in their so-called Uruguay Declaration, in which they advocated legally unobjectionable and transparent profiling.

The Resolutions and Declarations are available in English at: http://privacyconference2012.org/english/sobre-la-conferencia/noticias/noticia-destacada.

The 33rd International Conference in autumn 2011had appointed a working group to draft concepts for stepping up international cooperation between supervisory authorities. I am involved in the consultations representing Germany. The Privacy Commissioner of Canada (PCC) and the UK Information Commissioner's Office (ICO) have the chair of the group. In a next step Canada will present to the working group a concept for stepping up cooperation on data exchange and enforcing data protection vis-à-vis public authorities. The Canadian initiative is likely to be based on the idea that so far relevant agreements and coordinated actions have largely only existed at a bilateral level involving the EEA/Article 29 Working Party and the United States/Federal Trade Commission. However, the Madrid Declaration adopted at the 31st International Conference of Data Protection and Privacy Commissioners in 2009 already called for stronger international cooperation in the public sector (cf. 23rd Report, no. 13.14).

Beyond the International Data Protection and Privacy Conference, the Global Privacy Enforcement Network (GPEN) was set up as an informal association of national data protection authorities in spring 2010. Its goal is to improve international cooperation on enforcing data protection and privacy in the non-public sector. The Network was established in early 2010 on the initiative of the Federal Trade Commission (FTC) and has 31 members by now. Its work focuses on improving the mutual exchange of experience, carrying out training measures together with representatives of the private sector, academia and international organizations, and cooperation with comparable institutions. Bilateral support and cooperation measures can also be agreed, where appropriate.

2.4.4 Better cooperation between European data protection authorities

Data processing no longer stops at national borders. Data protection issues more and more frequently affect people in several Member States or across the whole of the EU. That means the data protection authorities need to step up cross-border cooperation.

The possibility and necessity of cooperation between national data protection authorities in regard to matters of a cross-border dimension were already established under the Data Protection Directive 95/46/EC. For example, Article 28 para. 6 provides that the supervisory authorities, “cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information”. In practice, such cooperation currently primarily occurs in the context of the Article 29 Data Protection Working Party and its subgroups, in particular the Technology subgroup (cf. no. 2.4.1.3).

As an example of fruitful cooperation between the data protection authorities in the context of this subgroup I would like to highlight the evaluation of Google’s new Privacy Policy which was undertaken in the course of 2012 (cf. no. 5.9). The evaluation was led by the CNIL, the French data protection authority. The subgroup was continuously involved in the technical analysis. Communication between Google and the CNIL, which acted on behalf of the Article 29 Working Party throughout the process, was also coordinated in consultation with the Technology subgroup. As a result of this cooperation the Article 29 Working Party forwarded a letter to Google on 16 October 2012 which was signed by the data protection commissioners of all 27 Member States.

I would like to mention the cooperation between the data protection authorities with the European Network and Information Security Agency (ENISA) on reporting data protection violations as another example of successful cooperation. The Technology subgroup and the ENISA are cooperating closely on developing a methodology for analysing the severity of privacy violations.

Finally, I would like to draw attention to the evaluation of the data protection policy of the social network Facebook (cf. no. 5.8.1). The Irish data protection authority being responsible tor the coordination, the Technology subgroup carried out a detailed assessment which led to two audit reports being drawn up.

The examples of “Google” and “Facebook” show how important it is that the data protection authorities of the EU Member States adopt the same policy in those cases in which people from several Member States or across the whole of the EU are affected.

The European Commission has taken up the globalization of data protection and in its Proposal for a General Data Protection Regulation suggests introducing a procedure of strengthened cooperation, administrative assistance and a consistency mechanism for cases in which several Member States are affected by the data processing of one controller (cf. no. 2.1.1). By means of a voting mechanism within the European Data Protection Board, the follow-up body to the Article 29 Data Protection Working Party, uniform legal interpretation and application are to be achieved within the EU in such cases. I explicitly support this goal. However, it must be ensured that the independence of data protection supervision remains unaffected and the data protection authorities remain in charge of the procedure. In addition, effective cooperation presupposes that the supervisory authorities have the necessary material and human resources at their disposal.

2.4.5 OECD and Council of Europe

Both the OECD and the Council of Europe are working to amend their data protection instruments. Although their efforts do not directly affect the stricter data protection rules in the European Union, the EU’s rules have inspired the discussion in the two organizations.

Their data protection instruments help strengthen and extend the reach of data protection not only due to their broad geographic range: The Council of Europe has 47 members and the OECD has 34. The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), which entered into force in 1981, was the first binding international instrument in the field of data protection. It spurred the development of a large number of national and international data protection initiatives. I am glad that the Council of Europe is planning to update Convention 108. The main objectives include amending it to meet new challenges to data protection arising from technological process and the Internet, such as cloud computing and the use of social networks, and ensuring that it is consistent with the EU’s data protection legislation, which is currently undergoing comprehensive reform (see no. 2.1).

I welcome the fact that, according to proposals for amending the Convention, its scope is to remain broad and coordination with data protection supervisory authorities is to be improved. The suggestions I made during the negotiations at expert level have largely been addressed. In particular, the provisions on cross-border data transfers now distinguish between data transfers among countries that are parties to the Convention and those that are not, while leaving room for stricter EU regulations. I expressly welcome this, because compatibility with the EU's draft General Data Protection Regulation is very important precisely with regard to cross-border data transfers.

The revision of the OECD's Privacy Guidelines from 1980 has been prepared by an expert group comprising government officials, staff of data protection supervisory authorities (including my office), scientists and representatives of industry, civil society and the Internet community. According to their proposal, the definitions of the Guidelines' basic terms, such as personal data, and the basic principles of data processing, such as purpose limitation and data security, should remain unchanged. However, the concept of accountability of data controllers is to be expanded and defined more precisely. Data controllers are to be obligated to fulfil the basic data protection principles defined in the Guidelines using a data protection programme. An important element of this programme is to be mandatory reporting of serious data protection violations, as also provided for in the draft EU General Data Protection Regulation. OECD member states will also be required to take further data protection measures at national level, including national data protection strategies and establishing independent data protection supervisory authorities. Lastly, the Guidelines require greater international cooperation on data protection, including measures to promote interoperability between different data protection systems as for instance with APEC (see no. 2.4.1.2). The OECD Guidelines represent only minimum standards (see Article 5 of the Guidelines). The OECD Council is planning to address the proposals for revision in spring 2013.

2.5 International data protection: Individual issues

2.5.1 SWIFT data to the US: Flying blind?

The conflict over transfers of SWIFT payment transaction data to the US continues. The reports of the Europol joint supervisory body add to doubts as to whether the restrictions built into the agreement are working. I find it scandalous that these classified reports are not presented to the national parliaments.

In 2006, US media revealed that US security authorities were using payment transaction data from SWIFT (Society for Worldwide Interbank Financial Telecommunication). Since then, such use has been the source of ongoing transatlantic conflict regarding the conditions under which sensitive data of non-suspicious individuals may be used for counter-terrorism purposes (see 23rd Report, no. 13.6).

In the past two years, the debate over the agreement between the EU and the US which entered into force on 1 August 2010 has focused on the extent to which data are sent across the Atlantic based on the agreement. Europol plays a decisive role in this regard, because the agreement assigns it a kind of monitoring role. SWIFT may not transfer any data from the EU to the US unless Europol confirms in each case that the specific US request for payment transaction data to be transferred meets the conditions of the agreement.

In my last report (23rd Report, no. 13.6), I noted the conflict of interest this causes for Europol. Europol's data protection inspections have confirmed my doubts concerning the agreement. The Europol joint supervisory body, in which staff from my office are represented, referred to the problems in its two public reports available at the time this report went to press.

The first report of the Europol joint supervisory body, which was published in 2011, stated that US requests were too abstract and too general, so that it was not really possible to check whether they complied with the agreement's requirement for requests to be kept to the minimum necessary. Further, key information justifying US requests was provided only orally; without documentation, it was therefore impossible to enter into examinations. The second report, published in 2012, also pointed out the difficulties in applying the agreement. Although the Europol joint supervisory body did note some progress, it remained unclear whether the European Parliament's demand to limit the amount of data transferred to the necessary minimum was met, because the Europol joint supervisory body is not allowed to publish specific facts and figures on the application of the agreement. The US had classified its requests as "secret" altogether before they were examined by the Europol joint supervisory body for the first time, and they retain this classification; for this reason, the Europol joint supervisory body was required to classify, in the same manner, as "secret" its complete reports on its controls.

This far-reaching classification complicates the reporting, discussion and evaluation of the agreement to a degree which I find incompatible with the principle of democracy. This classification means that even members of the national parliaments and of the European parliament are not supposed to receive this important information for evaluating the agreement. Ultimately, the European parliaments are responsible for evaluating the agreement, but they are not allowed to read the monitoring reports, not even in their document security offices precisely intended for such situations, and even though members of parliaments are known as the perfect bearers of secrets.

This is at least the view of Europol, the European Commission and the US government. As a result, classification by the US side means that European members of parliament are unable to find out about the practical implementation of the agreement, even though they bear political responsibility and are supposed to decide the extent to which financial data from Europe are transferred to the US. “Flying blind” this way cannot be allowed in a democracy. Thus the Europol joint supervisory authority has decided to provide the members of the European Parliament access to the complete monitoring reports in a way that complies with Europol’s regulations on security protection. It is clear that the last word in this conflict has not yet been spoken.

2.5.2 Passenger name records on and on

Airliners leave more behind than just vapour trails in the sky; airline passengers are generating ever-increasing data traces which do not, however, fade away. No wonder these data are such a hot commodity.

Whether and how passenger name records (PNR) collected by airlines for commercial purposes can be used, without reasons of suspicion, for threat prevention and law enforcement purposes has become one of the classic issues in the data protection debate at national and European level and, above all, in the transatlantic relationship with the US. During the reporting period, the focus was on two developments: agreements with the US and Australia (see no. 2.5.2.1) and the proposal for an EU directive authorizing the European police authorities to collect and process PNR data for law enforcement purposes without specific reason (see no. 2.5.2.2).

2.5.2.1 Transferring passenger data overseas

The extensive transfer of European passenger data to the US is continuing on the basis of a new agreement. More and more countries are following this model. My critical view of this has not changed.

For more than ten years, US security authorities have demanded a multitude of personal passenger data at different times from a variety of sources before every flight to the US, and they use these data for counter-terrorism and other purposes (see previously 23rd Report, no. 13.9). Even specialists meanwhile have a difficult time keeping track of all the different requirements for data transfers. The most sensitive are probably those for passenger name record (PNR) data collected by airlines for the purpose of conducting flights. PNR data include credit card and telephone numbers, e-mail and contact addresses and special meal requests.

Since summer 2012, PNR data have been transferred on the basis of a new agreement between the EU and the US. The EU also negotiated a new agreement with Australia on the transfer of PNR data. I criticized the agreement with the US in particular, not only in principle but also with regard to various details. The central criticism in the opinion of 6 January 2012 by the Article 29 Working Party, to which I made a significant contribution, is still the long retention period of 15 years for all data.

I view as an improvement that data can now be accessed, as a rule after a certain time, only by means of a mask. However, this does not change the fact that all the data are stored in their entirety for the entire retention period. The agreement also leaves many unresolved questions with regard to the purposes for which the data may be used. Nor am I satisfied with the possibilities for legal redress for European citizens under US law. In comparison to earlier or comparable agreements, the new agreement contains more references to various US statutes, but major doubts remain as to whether they really provide legal redress for Europeans assimilated to that of US citizens. In any case, data subjects who are not US residents have no right under the PNR agreement to request a judicial review of the storage and processing practices of the US authorities.
I believe it is doubtful whether the PNR agreement allows the transfer of PNR data to the US from flights that merely fly over the US without landing there. The US authorities demand that airlines also supply passenger data from flights that only touch US airspace, such as direct European flights to the Caribbean.

Finally, I note with concern that more and more countries are demanding the prior transfer of extensive passenger data on the US model, including countries which can hardly be considered democracies. I am anxious to hear the responses from Berlin and Brussels.

2.5.2.2 PNR for Europe?

The European Commission has moved in the direction of groundless storing of passenger data.

Will European security authorities, too, use and store PNR data without specific suspicion? The European Commission presented a new proposal in February 2011 which provides for this. The Council has argued over this project for many years. The first proposal in this direction was made in November 2007 (see 22nd Report, no. 13.5.3), but was heavily criticized and not pursued further.

In its resolution of 16-17 March 2011, the conference of the data protection commissioners of the Federation and of the Länder made clear the critical points (see box for no. 2.5.2.2). According to this, the new proposal, too, fails to provide concrete evidence that groundless automated analysis and evaluation of airline passenger data by police and law enforcement authorities is appropriate and necessary to fight terrorism and serious crime.

Further, the proposal challenges the rulings of the Federal Constitutional Court (*Bundesverfassungsgericht*) in two respects: First, storing all PNR data without reasonable suspicion would constitute further groundless data retention, this time not by providers of telecommunications services, but directly by border or police authorities. In its judgment on groundless data retention (judgment of 2 March 2010, 1 BvR 256/08), the court made it clear that the individual exercise of freedom of action may not be recorded and registered in a total manner, stating that this belonged to the constitutional identity of the Federal Republic of Germany (see 23rd Report, no. 6.1). So the chances for groundless data retention are very limited, not only in terms of data protection policy, but also in terms of constitutional law.

The other constitutional law issue has to do with the plan to check the data of each passenger against predefined risk profiles. The similarity to computer-aided profiling and search is obvious. But according to the decisions of the Federal Constitutional Court, preventive computer profiling and search is prohibited unless there is a

sufficiently concrete threat to high-ranking protected interests (decision of 4 April 2006, 1 BvR 518/02; see 21st Report, no. 5.2.3).

Another major point of dispute concerns a provision which is not even included in the Commission's proposal: Certain Member States and members of parliament also want to include flights within the European Union, thus not only long-distance flights, but also flights between Berlin and Paris or Cologne and Rome. Then it would only be logical to include the data of rail, ship and bus passengers, too. This is how the culture of surveillance spreads, just like an oil slick on the water. One can only hope that constitutional law "oil barriers" will keep this trend from spreading.

Box for no. 2.5.2.2

Resolution of the 81st Conference
of the Data Protection Commissioners of the Federation and of the Länder
of 16/17 March 2011

No retention and screening of air passenger data!

On 2 February 2011 the European Commission presented a new proposal for a directive on the use of EU air passenger data for the prevention of threats and for law enforcement purposes.

The focus of the draft is the systematic collection of the data of all passengers crossing the EU's external borders. Irrespective of causes and suspicions, it is intended to transfer these data from the airlines' reservation systems to a national central office of the law enforcement authorities and to store them regularly for a five-year period. This shall allow to identify persons who could be involved in terrorism or serious crime.

Also the new draft does not provide concrete evidence that the automated processing and analysis of air passenger data without any cause is appropriate and necessary in order to support this objective. Such a combination of retention and

screening of passenger data is neither compatible with the EU Charter of Fundamental Rights nor with the constitutionally guaranteed right to informational self-determination. This is particularly true with regard to the jurisdiction of the Federal Constitutional Court, which in its ruling of 2 March 2010 (1 BvR 256/08) on the retention of telecommunications data called to mind the following fact:

It is a part of the constitutional identity of the Federal Republic of Germany that it is not allowed to completely capture and register the citizens' exercise of freedom. The Federal Republic of Germany has to stand up for this issue also at the European and at the international level.

Such a system would allow even farther-reaching encroachments upon civil rights if even proposals for the retention of air passenger data for flights within the European Union and of data of rail and boat passengers were included in this directive.

This draft shows again clearly that a coherent overall concept at the European level for data processing in the field of internal security, which sufficiently guarantees the data subjects' fundamental rights, is lacking.

Therefore, the Conference calls on the Federal Government and the Bundesrat (Federal Council) to advocate that the European Commission's proposal for a directive on the use of passenger data will not be put into effect.

2.5.3 On the future of border and aviation security controls

Border and security controls are no fun for anyone; they are annoying and time-consuming. After being reduced everywhere for decades and entirely discontinued within the Schengen area, they have been undergoing a renaissance especially since the terrorist attacks in 2001. No wonder that technology is increasingly being applied.

Both the aviation industry and politicians have been enthusiastically dreaming up new ideas. The International Air Transport Association (IATA) has made its ambitions clear in the title of its large scale project: creating the "Checkpoint of the Future" (see 23rd Report, no. 7.3.2). The Federal Ministry of the Interior is also working on new strategies for aviation security. The renewed roll-out of full-body scanners is just one

measure; other plans include further developing biometric border controls and programmes for so-called registered frequent travellers. Even the European Commission has also started thinking about “smart checks”.

2.5.3.1 “Checkpoint of the Future”: A discrimination trap?

In the airport of the future, security checkpoints are supposed to identify “high-risk passengers”. This will necessarily lead to unjustified intensive controls and to discriminatory practices, and whether this will really improve security is questionable.

In my last report I described IATA’s initial and still-vague plans to create a model for the “Checkpoint of the Future” (23rd Report, no. 7.3.2). According to the now more developed plans, “risk-based security screening” is supposed to be able to process more passengers in less time. In addition, more and more travellers are to be enrolled following a background check as registered travellers in the appropriate programmes.

The IATA’s new strategy raises many question, above all: How will it find out who is a “high-risk passenger” as the main focus of security screening shifts away from identifying dangerous objects?

So it is obvious that passengers will be subject to comprehensive profiling and monitoring of their behaviour at the airport. According to the IATA, data from airlines and security authorities would also play a key role.

But the IATA’s strategy leaves a number of questions unanswered: What assumptions will the decision be based on? Who will supply, analyse and store the analyses, conclusions and facts for this new kind of risk assessment or “scoring”? And who will decide which passengers might be high-risk? The Article 29 Working Party has addressed this important issue and is currently discussing exactly these questions with the IATA.

I am extremely sceptical about the new orientation of the IATA model. Does the motive of cost-effectiveness justify checking every passenger against all possible police databases, and in addition to that, against abstract risk profiles? Is it even possible to objectively assign each passenger a risk score between 1 and 5 or 1 and 10 without discriminating against and violating the rights of personaltiy? According to the IATA, the global implementation of the project will differ depending on the

applicable law, as the legal use of personal data is ultimately determined by national standards. So there will not be one “Checkpoint of the Future”, but many.

If the plans for the “Checkpoint of the Future” gain acceptance, the current equal treatment of all passengers (“one-size-fits-all”) will no longer apply. High-risk travellers, unregistered infrequent travellers, members of certain ethnic or age groups and citizens of certain countries would face more intensive controls than today, while high-value business travellers and other frequent fliers would more or less be waved through. I doubt whether this scenario is compatible with our notions of the right of personality, of fundamental and human rights. I also question whether such a system would really provide greater security, as it would encourage terrorists to infiltrate the group of registered frequent fliers subject to less screening.

In any case, I will work to ensure that passengers’ rights of personality will not crash when it comes to the airport security of the future.

2.5.3.2 From nude scanners to full-body scanners

The Federal Ministry of the Interior tested full-body scanners for ten months, against the backdrop of intense public debate. The machines were found to be too unreliable and sent back for further research. Now devices with updated software are being used.

The test of full-body scanners was a focus of my last report (23rd Report, no. 7.3.1). The Federal Ministry of the Interior set up one full-body scanner at a German airport as an experiment. After ten months of testing at Hamburg Airport, it found that the machines were still too unreliable and sent them back to the Federal Police research centre.

Passenger participation in the test was voluntary, to which I had attached great importance. The devices largely met the conditions agreed on in a resolution of the conference of the data protection commissioners of the Federation and of the Länder (published in the 23rd Report, p. 89). In particular, it was important that the devices used did not generate any images of actual bodies, unlike earlier models, called “nude scanners” by the news media. The Federal Ministry of the Interior informed me that it agreed with these requirements. Instead, the latest full-body scanners use pictograms (stylized stick figures) onto which a clearly visible object is projected.

Full-body scanners have been in use again for security screening since December 2012, this time at Frankfurt Airport. Once again, no one is forced to undergo a full-body scan. Every passenger has an alternative to security screening with a full-body scanner. I do not yet dispose of concrete results or findings of my own on these devices. The decision to use them again was made shortly before this report went to press. The Federal Police have informed me that the devices are the same type as was used in Hamburg. I will continue to monitor their use and check their design and local operation to see whether they comply with data protection requirements.

2.5.3.3 The future of biometric border controls

The Federal Ministry of the Interior wants to consolidate the existing projects on biometric border controls.

The Federal Ministry of the Interior is planning to update the biometric border controls at German airports. I, too, believe consolidating the current projects is a good idea. There are currently two biometric recognition procedures in operation at Frankfurt Airport.

In one, the Automated and Biometrics-Support Face Recognition (*automatisierte biometriegestützte Gesichtsekennung* (ABG)), travellers who have voluntarily registered ("registered travellers") with the programme are identified using iris recognition: The iris is scanned and checked against an image of the traveller's iris stored locally with his or her permission (see 22nd Report, no. 4.5.2 and 23rd Report, no. 3.5). In the other project, "EasyPass", EU citizens with biometric travel documents can choose automated border controls in certain security lanes using facial recognition. Their face is checked against biometric data stored in the passport, so that no additional local storage of the facial image is necessary (see 22nd Report, no. 6.4 and 23rd Report, no. 3.5).

Both projects largely meet the technical requirements for data security.

However, I had concerns regarding their legality. Legislation has defined fingerprints and facial images as the only form of biometric identification permitted in official identification documents, making iris recognition obsolete. Further, the Schengen Borders Code defines how Member States are to carry out border controls at the external borders of the Schengen area. For flights entering the Schengen area, these border controls take place at Frankfurt Airport. According to Article 7 (2) of the

Schengen Borders Code, EU citizens may not be required to undergo a systematic database query when entering the Schengen area. But both the ABG and EasyPass are set up to conduct a full query of every passenger going through the screening. In my view, this practice violated Article 7 (2) of the Schengen Borders Code.

The Federal Ministry of the Interior noted my comments when revising the biometric border controls and announced that it would combine the ABG and EasyPass under the EasyPass-RTP (Registered Traveller Programme) and discontinue the iris checks. The plan is to open EasyPass security lanes at the five busiest airports by the end of 2013. By the end of 2014, the security lanes are to be enhanced so that they can accommodate entering third-country nationals, by means of an automated border control, who have undergone a prior background check and registered with the programme. Then both EU citizens and registered non-EU citizens can use the same automated security screening. In order to comply with Article 7 (2) of the Schengen Borders Code, the EasyPass security lanes will be equipped with a randomizer.

I welcome the Federal Ministry of the Interior's announcement. I will continue to monitor the progress of this project.

2.5.3.4 "Smart borders": Not particularly intelligent

Under the heading "smart borders", the European Commission is planning to set up an entry/exit register and wants to improve the programme for "registered travellers". I am especially critical of the planned register, which is supposed to record every border-crossing of a non-EU national.

The European Commission says that the EU's external borders need to become "smarter". It sketched out the general outlines in its Communication of October 2011: "Smart borders" means keeping an electronic record of the entry and exit of non-EU citizens and making it easier for them to enter the EU if they register and undergo a prior background check. Non-EU citizens will not be required to register before entry, however, as it is the case for non-citizens entering the US under the Electronic System for Travel Authorization (ESTA).

I am especially critical of the basic item of the considerations, embodied in the entry/exit register. It represents an enormous database recording every time a non-EU national is crossing the EU's border, independent of whether he or she needs an

entry visa or not. The European Commission argues that the register will make it possible to monitor border crossings more effectively and adds that there are currently no reliable data on the number of persons overstaying their visas (so-called overstayers) and remaining in the EU longer than allowed. According to the Commission, this is a major problem, as “overstayers” constitute the main source of irregular immigration in the EU.

I doubt whether it is even possible to create and administer such a system without unreasonable effort given the many land and sea borders in Europe. The US, with its much more controllable borders, started building such a system years ago, so far without noticeable success. Apart from the feasibility of such a system, I cannot see anything to justify the necessity and proportionality of a database on this scale; precisely with regard to so-called overstayers, it is not clear what concrete benefit the system could provide. Simply yielding more accurate statistics on irregular immigration would not be enough to justify this measure.

The second component of the “Smart Borders” initiative after the entry/exit register is the Registered Traveller Programme (RTP) for frequent travellers. In the Commission’s view, it would not make sense to subject all non-EU nationals entering the Schengen area to the same screening. Entry for frequent travellers could be facilitated if they register and undergo a background security check before their journey. Here is the concrete point of contact with the “Checkpoint of the Future” (see no. 2.5.3.1) and the Federal Ministry of the Interior’s EasyPass-RTP (see no. 2.5.3.3).

According to current plans, both systems will provide for biometric identification. So it remains to be seen what the draft legislation actually says and how the requirements of data protection law can be met, especially with regard to avoiding excessive preventive retention of data.

Finally, I would like to raise a heretical question: Is it really smart to have only one response to all the possible security threats: additional data storage, comprehensive registration and preventive profiling?

2.5.4 Data protection trends in the US

A policy paper presented by the US government contains a “Consumer Privacy Bill of Rights”. The Federal Trade Commission (FTC) published a report with

recommendations on data and consumer protection in a networked world. But there are still almost no binding data protection rules for the private sector in the US.

In February 2012, at nearly the same time the European Commission presented its proposals for EU data protection reform, the US government published the white paper "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy". The paper contains a summary of consumer rights in a digital world ("Consumer Privacy Bill of Rights") with seven basic requirements for the processing of personal data: information, purpose limitation, necessity/data minimisation, data subjects' rights, responsibility/accountability and data security. The Obama Administration would like to see the Consumer Privacy Bill of Rights enacted by the Congress in the form of federal legislation. But no action to this end has been taken since then, neither in the US Senate nor in the House of Representatives. Nor has the Congress granted the FTC the necessary powers to enforce these rights as called for in the white paper.

The draft largely relies on self-regulation and does without the kind of binding data protection rules which are provided for in EU data protection law and are to be maintained according to the Commission's proposals (see no. 1.1). In this sense, the US government proposes that in the framework of "multi-stakeholder" procedures codes of contact are elaborated in the various sectors in order to concretise the rights guaranteed in the Consumer Privacy Bill of Rights. International partners such as the European Union should also be included in the process of drafting legally binding codes of conduct. In this way, more specific codes of conduct could possibly be added to the Safe Harbor legal framework.

In 2012 the FTC published the report "Protecting Consumer Privacy in an Era of Rapid Change". In this report, the FTC recommends both elaboration and application of best practices for businesses, such as privacy by default and privacy by design, as well as giving consumers greater control over their data, for example by simplifying choices and increasing transparency.

The FTC sees a particular need for action in the following areas:

– do not track (integration in Web browsers)

– mobile services (better information for consumers)

– data brokers (greater transparency concerning their processing of data)

– large platform providers (risk of comprehensive tracking)

– sector-specific enforceable self-regulatory codes to be developed by the Department of Commerce with the support of key industry stakeholders. This serves to implement the white paper of the US government (see above).

The FTC's report also calls on Congress to enact clear legislation for businesses to ensure that the application of data protection solutions does not result in economic disadvantages. It also calls for rules on data security and data loss as well as appropriate consumer access to information about them. I expect that the FTC will continue to pursue these goals, even though Congress has not yet addressed them.

I will continue to maintain my good contacts at the FTC developed through several visits and return visits in 2011 and 2012. It would be desirable, however, if, beyond its certainly worthwhile proposals and announcements, the US would adopt binding data protection rules ensuring the same level of protection long provided in Europe. This would not only be in the interest of citizens on both sides of the Atlantic; it would also encourage the transatlantic exchange of information and data, for example in the context of cloud services (see no. 5.3).

2.5.5 Foreign Account Tax Compliance Act (FATCA)

To implement FATCA, EU Member States including Germany drafted a model agreement with the US which also covers data protection.

The implementation of FATCA has created significant problems of data protection (see box for no. 2.5.5). For example, the question was raised whether the transfer of data to the US Internal Revenue Service (IRS) is permitted on the basis of Sections 4b and 4c of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) or on the basis of consent. Clarification is to be provided by bilateral agreements between the US and five EU Member States (France, Italy, Spain, the United Kingdom and Germany). A model agreement was presented on 26 July 2012 in which the five countries agree to collect information on accounts held by US citizens at financial institutions on their territory and provide it to the IRS. In return, the US agree to free all financial institutions in each of the five countries from the obligation

of concluding agreements with the IRS in order to avoid having US tax withheld at the source under FATCA.

This model agreement creates a framework for the financial institutions to report certain account data to their tax authorities; these data are then shared in the framework of existing bilateral double taxation conventions. The Federal Ministry of Finance is currently preparing the bilateral agreement between Germany and the US. Further, national legislation allowing financial institutions to transfer data to the national tax authorities is being drafted. The Federal Ministry of Finance included me in the drafting process from the start, and I have worked to ensure an appropriate level of data protection.

The Article 29 Working Party of the European data protection commissioners has also addressed this issue. In a letter of 21 June 2012, the group's chair wrote to the European Commission's Directorate General Taxation and Customs Union (TAXUD) to point out the data protection problems related to FATCA.

According to the current state of negotiations, a provision covering the purpose limitation principle is to be included in the agreement itself. Contrary to my wishes, however, the procedural safeguards along with the technical and organizational data security measures will be covered in a separate implementing agreement.

Box for no. 2.5.5

Foreign Account Tax Compliance Act (FATCA)

The Foreign Account Tax Compliance Act (FATCA) is a US law effective as of March 2010 to gather information on assets outside the US belonging to persons and organizations subject to US taxes.

The core of FATCA lies in that it requires banks and other foreign financial institutions (FFIs) to report information on an enlarged scale to the US Internal Revenue Service (IRS). Tax-related information on US citizens must be provided to assist in the investigation of tax-related crimes. In addition to accounts, securities and shares deposited with banks which are already covered by so-called qualified intermediary agreements, the new law also covers investment funds and certain types of insurance such as pension and capital sum life insurance.

FATCA requires all FFIs, on the basis of an agreement with the IRS, to check their clients' accounts for possible tax liability in the US and, with the client's consent, submit to the IRS regular and detailed reports concerning taxable accounts and payments. Relevant data include name, address and US tax number of the clients concerned as well as transaction data and account balances. US clients must explicitly consent to this infringement of banking secrecy by the US authorities and have to waive bank secrecy in a compromising manner at the favour of US authorities. If they do not, the financial intermediaries must discontinue their businesses with these clients. The new law affects not only US citizens living in Germany, but also Europeans subject to tax in the US.

If FFIs fail to report, the IRS withholds taxes of 30% (tax withholding at the source) from all payments to the FFI based on US assets. Thus FATCA forces FFIs worldwide to choose between giving the US authorities access to personal data of US clients, or facing a tax (withheld at the source) on their profits from US securities.

3 Basic matters

3.1 Independence of data protection authorities

The judgment of the European Court of Justice of 16 October 2012 on the lack of independence of the Austrian Data Protection Commission is largely applicable to my legal status.

Already in 2010, the European Court of Justice ruled in an infringement proceeding that the organization of German data protection supervisory authorities in the private sector at state level did not meet the requirement of the Data Protection Directive 95/46/EC of "complete independence" (ruling of 9 March 2010, C-518/07 – see 23rd Report, no. 2.1). According to the court, the independent status of the data protection authorities is intended to guarantee that they can exercise their functions free of outside influence. Any kind of political or institutional influence, such as government supervision or even the appearance of government influence, would be incompatible with this requirement. The German states (Länder) have since revised the legal status of their data protection supervisory authorities for the private sector to comply with the court's ruling.

In the public sector it is even more important than in the private sector that the executive should have no influence over the supervisory authorities in perform their duties, since the executive on its part is controlled by them. The Federal Ministry of the Interior has not yet taken any action as the result of this ruling.

With its judgment of 16 October 2012 (C-614/10), the European Court of Justice confirmed its ruling on the need for “complete independence” of the data protection authorities and expanded this to the public sector for the first time. The subject of the infringement proceedings initiated by the European Commission was the legal status of the Austrian Data Protection Commission (*Datenschutzkommission*, DSK), which is responsible for monitoring data protection in both the private and the public sectors in Austria. The Federal Republic of Germany joined the proceedings as an intervener in support of Austria.

It is not surprising that in the proceedings against Austria the European Court of Justice once again stressed that the requirement of complete independence for the data protection authorities is to be understood in a comprising sense: According to the court, “complete independence” means ruling out not only direct influence in the form of instructions, but also every form of indirect influence by state agencies which would be able to steer the decisions of the data protection authority. The court said that among other things, the fact that the managing member of the Austrian DSK was a federal civil servant subject to administrative supervision was incompatible with such independence. The court said that it could not be excluded that the managing member of the DSK might be influenced in his decisions by the federal agency responsible for administrative supervision. The court also criticized the DSK’s organizational status as part of the Federal Chancellery, which under Austrian law provides the DSK’s material and personnel resources. Because the DSK office employs civil servants assigned by civil service law and civil service remuneration law to the Federal Chancellery who are thus subject to its administrative supervision, the decisions of the DSK are at risk of being influenced, as the DSK is ultimately responsible for monitoring the Federal Chancellery.

Even though the Federal Republic’s joining the proceedings as an intervener in support of Austria has no direct legal effect for Germany, the ruling sends a clear signal. The legal status of Germany’s Federal Commissioner for Data Protection and Freedom of Information as provided for in the Federal Data Protection Act is similar in many respects to the legal situation in Austria that the court objected to: Germany’s Federal Commissioner is subject to legal supervision by the Federal

Government and to administrative supervision by the Federal Ministry of the Interior. And in organizational terms, the Federal Commissioner's office is located at the Federal Ministry of the Interior. The Federal Commissioner's staff are employed by the Federal Ministry, which has a say in hiring and promotion and is responsible for their administrative supervision.

In order to avoid having to be told a third time by the court, the Federal Republic of Germany should change the Federal Commissioner's legal status in order to comply with the requirement of complete independence. Until this happens, the existing legal provisions must be understood in terms of the complete independence required by European law. I am discussing this issue with the Federal Ministry of the Interior.

4 Technological data protection

Data protection is largely a response to technological challenges. That is why there is probably no topic in this report where information technology does not play a role. This chapter deals with projects and topics in which technological issues are central, such as major projects like the electronic health card and the ELENA project on processing electronic wage statements which was recently killed. This chapter also deals with horizontal technical issues which come into play almost everywhere, such as requirements for the secure erasure of data.

4.4 Technical standardization ever more important

Along with legal provisions, technical standards are becoming increasingly important for data protection. I am involved in drafting these standards.

Standardizing technical architectures and processes as the basis for technical data protection requirements is becoming more and more important. The draft General Data Protection Regulation also includes many references to setting technical standards (see no. 2.1.1). For this reason, I am increasingly contributing to standardization projects at international and national level.

Technical standards have gained acceptance in many areas of IT security. With their direct connection to technological data protection, these standards necessarily touch on technical aspects and those of data protection law. So it is all the more important to take part in the development of standards at an early stage in order to have the greatest possible influence on the result.

At national level, I am currently participating in the efforts of the German institute for standardization (*Deutsches Institut für Normung* (DIN)) to draft and revise standards for the following:

– the destruction of storage media (DIN 66399) (see no. 4.6),

– cards and personal identification (NA 043-01-17 AA) and

– biometrics (NA 043-01-37 AA)

(see 23rd Report, no. 5.3).

In addition to supporting interoperability and data exchange between applications and systems, the standards for “cards and personal identification” and for “biometrics” primarily have to do with including national interests into international standards. By participating in these DIN bodies, I hope to ensure that aspects of data protection, such as protecting the private sphere in biometrics, are better anchored in these technologies. In doing so, I am working closely together with the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* (BSI)). I also help advise on new projects to be standardized, such as drafting standards for erasing data (see no. 4.5).

International standards are gaining in influence as part of the reform of European data protection law (see no. 2.1) and the increasing acceptance of data protection-friendly concepts such as privacy by design and privacy impact assessment (PIA). At international level, the International Organization for Standardization (ISO) has established a task force to deal exclusively with the issues of “identity management” and “technological data protection” and to draft, inter alia, standards for privacy impact assessment and cloud computing, among others. It is very difficult to set global standards for data protection, in part because the standards must accommodate not only the regional German (and European) data protection requirements, but also a number of wishes of other countries and regions. So my basic position is that ISO standards should only address overarching data protection issues. Initial approaches are being drawn up in the project on ISO 29100 (“privacy framework”).

Here I see the possibility to standardize basic principles and a framework architecture for technological data protection.

However, I am in favour of keeping these as general as possible and dealing with aspects of European data protection within the European standards organizations. For example, a CENELEC (European standards in the field of electrical engineering) standard would be conceivable here. Together with ETSI (telecommunications standards) and CEN (standards for all other technical areas), CENELEC constitutes the European system for technical standards and would be the appropriate body to set standards for specifically European aspects of data protection.

With regard to the unbelievable speed with which new technologies arise and become obsolete, standardization projects must become less bureaucratic and the process of developing standards must be streamlined. Otherwise standardization will lag behind constant technological progress.

The importance of technical standards will continue to increase in future. I will continue to participate in standardization projects and will work even more closely in efforts at national and international level, also in the course of future developments concerning the General Data Protection Regulation.

4.5 Data erasure: A guideline

It is not always easy to erase digital data. Sometimes, however, those who are responsible lack the necessary knowledge or willingness to deal with legal provisions on data erasure.

Data erasure is increasingly important in a digital world. Although it is easy to destroy paper, getting rid of digital media is often problematic, partly because data with different retention schedules are stored, in a highly integrated manner, in databases and because the deletion process must pay attention to a variety of links. In these cases, IT solutions can help which keep track of legally mandated data erasure from the beginning.

But sometimes, those responsible for IT procedures see no reason why they should delete data once they are stored – after all, limited data storage capacity is a thing of the past. And sometimes the problem is simply a lack of awareness.

I support the private sector’s efforts to standardize the data erasure process; I advised on drafting a respective guideline.

The federal administration is also increasingly moving from paper-based processing to digital (see also on digital personnel files, no. 13.3). The shift from paper to electronic processing usually gives rise to a new problem: data erasure. For many business processes and IT applications process personal data which are subject to data protection regulations.

The data protection principles of necessity, data reduction and data economy state that data must be deleted once they are no longer needed. For example, Article 6 of the 1995 EU Data Protection Directive contains rules on erasing and anonymizing data. Articles 20 (2) and 35 (2) of the German Federal Data Protection Act (*Bundesdatenschutzgesetz* (BDSG)) require that data are to be erased when they are no longer needed for the purpose for which they may lawfully be used. These principles are referred to in ISO 29100 (see no. 4.4) as “data minimization” and “use, retention and disclosure limitation”.

In practice, legal regulations on data erasure are often inadequately implemented, running in particular into the following problems:

– data controllers regard erasure requirements as unnecessary or too expensive;

– erasure would make it impossible to use the data at a later time for some as yet undetermined purpose;

– technical systems often fail to provide for complete and irreversible data erasure;

– controllers have a difficult time determining the end of processes for data collections and thus setting concrete deadlines for erasure;

– many of those involved must understand highly differentiated erasure rules in order to carry out the erasure mechanisms in the relevant IT systems; and

– there is no clear understanding of how to monitor and document the proper implementation of the erasure regulations.

In order to ensure that personal data are erased as required by law and in an orderly fashion, controllers must develop rules and assign responsibilities. Establishing such a strategy for erasure is a complex and comprehensive task. The chances of developing a successful and specific strategy for erasure could be improved if

controllers had a reliable model of methods and design to fall back on. The guideline proposes a way to establish a corporate strategy for data erasure.

The DIN is exploring the possibility of making the guideline an international standard. The guideline helps controllers fulfil their legally mandated duties to erase personal data. It provides recommendations for the content, structure and assignment of responsibility in a strategy for erasure which complies with the principles of data protection. The methods and structuring proposals can be used by all controllers. The guideline is aimed primarily at those responsible for data protection and at persons involved in developing an erasure strategy. The guideline is published on my website, www.datenschutz.bund.de.

An erasure strategy can be established with reasonable effort only if all those involved can understand the rules on erasure and if the requirements are not excessively complex. Simple rules are therefore the key to success. This is why the guideline recommends using standardized retention periods and “erasure classes” which can be adapted to the specific organization as needed. These “erasure classes” reduce the complexity of the various requirements and constitute the core of the erasure strategy. They are used to assign collections of personal data to erasure rules. An erasure strategy of the kind proposed here has a variety of benefits for a controller:

– It helps to protect data subjects for the purposes of the right of personal self-determination

– The controller meets its legal obligations and can demonstrate its compliance with data protection regulations as regards erasure obligations.

– Processes are more clearly determined, because the obligation to erase means that their ends have to be defined.

– Data storage is systematized and consolidated, because archives are also subject to erasure and thereby purged, which includes reducing the cost and effort of data migration when the switch to new IT systems is made.

– Purging data collections and reducing unnecessary redundancies can reduce the cost of IT operations.

– The erasure strategy sets goals for the erasure of data collections which can easily be turned into criteria for audits.

– The systematic recording of personal data gives those responsible for data protection an overview of data collections and the relevant systems.

– And the discussion of erasure rules and the constructive organization of business and IT processes anchors data protection more firmly within the controller.

The guideline also includes definitions of key terms needed in the discussion of erasure rules. They facilitate understanding among expert users, those responsible for IT, system developers, management, those responsible for data protection and other stakeholders. Rules for implementing the proper erasure of personal data in IT systems can even be helpful when designing business processes. They can help define erasure requirements for system development and acquisition processes. The guideline also informs software makers how IT systems can support the controllers' task of erasing personal data.

I hope that stakeholders will make use of this possibility to address the question of erasing data in digital systems or processing digital files and will draw the necessary conclusions.

4.6 Destruction of data storage media: New DIN standard 66399 adopted

The new DIN standard on the destruction of data storage media (DIN 66399) published in September 2012 allows controllers as the "master of data" to determine classes of protection and security levels flexibly and to choose the method of destruction appropriate to their needs.

The new DIN 66399 replaces the previous DIN 32757. I noted in the 23rd Report (no. 5.3) the problems with media destruction that arise due to modern technologies, newer materials, recycling and environmental considerations. The main results of lengthy meetings with representatives of the waste disposal industry and device manufacturers are as follows:

– Data are broken down into three protection classes

Determining the need for protection and assigning the protection class and the security levels serve to classify the data generated.

– Six categories of material
The standard for the first time defines different categories of material and takes into account the amount of information stored on the medium. The standard distinguishes between paper documents, optical, magnetic and electronic storage media, and hard drives.

– Seven security levels
Instead of the previous five levels of security, the new DIN 66399 now defines seven security levels. A key difference is the new level P-4 with a particle surface of max. 160 mm^2.

– New storage media
The new standard is the only one anywhere in the world which offers a comprehensive guide to destroying “new media” (such as CDs, DVDs, hard drives, USB sticks and memory cards). By introducing two additional security levels which are to take into consideration technical development, the current standard also takes account of future developments.

The new standard defines both the requirements for machines to destroy storage media and the related processes, making DIN 66399 the most comprehensive and complete standard concerned with the destruction of data storage media. Together with the national institute for standardization I hope to establish this standard at international level.

5 Internet

5.1 Right of information under Section 101 of the Copyright Act: Show me your IP and I’ll tell you who you are

The Federal Court of Justice (Bundesgerichtshof (BGH)) decision on the conditions of the right of access under Section 101 of the Copyright Act is likely to result in more

customer data being sent from Internet access providers to right holders. Legislators are called on to review the statutory regulations.

I continue to receive petitions from individuals who are being warned with costs for allegedly downloading files from the Internet illegally. In certain cases, the warning fees can add up to several thousand euros. The warning notice informs the subscribers that right holders were given their addresses by their Internet service providers. In case of suspected copyright violations, customer data of subscribers may be disclosed to right holders on the basis of a court order. If Internet service providers release customer data (name and address) to right holders on the basis of a court order, this is not problematic in terms of data protection law (see 23rd Report, no. 4.8).

Nonetheless, I remain critical of the developments in this area. Companies hired by right holders use special software to systematically search Internet file-sharing sites for copyright violations. There is no specific legislation in this regard. However, the courts regard it admissible to identify IP addresses of possible copyright violators by automated means.

Further, the conditions under which Internet service providers can be required to provide information have been further relaxed, based on a Federal Court of Justice (*Bundesgerichtshof* (BGH)) decision published on 10 August 2012 concerning the prerequisites for Sect. 101 of the Copyright Act (*Urheberrechtsgesetz* (UrhG)) (I ZB 80/11). During the legislative process to introduce the right of information, I argued that this right should be limited to serious cases (see 21st Report, no. 6.5). The new Section 101 of the Copyright Act created a complicated provision on the right of information, and the courts have disagreed on the conditions for this right. Some courts found that issuing a court order depended on the suspicion of “legal violations in commercial quantities” and rejected applications by right holders when, for example, older songs were concerned. Since the Federal Court of Justice decision, it is no longer necessary to examine the seriousness of a violation; the suspicion of a simple violation suffices.

Because lower courts will base their decisions on that of the Federal Court of Justice, the number of requests for information is likely to increase. So it is necessary to ask whether this legal situation represents an unreasonable intrusion into subscribers’ secrecy of telecommunications. In my view, the right of information should be limited

to serious violations of the law. I therefore recommend that legislators should review the current law and amend it with the principle of proportionality in mind.

5.2 “ACTA” – ad acta!?

Following Europe-wide protests, on 4 July 2012 the European Parliament voted by a large majority to reject the Anti-Counterfeiting Trade Agreement (ACTA). This agreement will not enter into force in the foreseeable future.

In my 23rd Report (no. 4.7), I referred to the negotiations on ACTA, which was available in its final version from December 2010. When it became known that the European Union and 22 of its member states had signed ACTA on 26 January 2012, criticism of the agreement grew. ACTA critics worried that copyright law would be made stricter, to the detriment of Internet users. In particular, they feared Internet censorship, blocking on the “three strikes model” and monitoring of Internet traffic.

Their criticism was certainly justified, as the final text of the agreement contains many unspecific provisions. Although the provisions do not contain any concrete obligations to amend existing law, they do leave a great deal of room for interpretation, extending to obligating access providers to monitor and filter Internet traffic. Thus the provisions could have been used as a pretext to advocate stricter enforcement of copyright at the expense of freedom of information and data protection.

Following the massive public criticism, in February 2012 the Federal Ministry of Justice (Bundesministerium der Justiz (BMJ)) announced that Germany would not sign the agreement for the time being. And the European Commission said that it would ask the European Court of Justice to review the agreement for its compliance with the European fundamental rights. But this review was ultimately irrelevant, as the European Parliament decided not to postpone its vote on ACTA until the court had presented its results and voted against ACTA on 4 July 2012. As a result, the EU member states can no longer accede to the agreement.

The end of ACTA for sure is not the last word on efforts to achieve international agreements to enforce intellectual property rights. Unlike this failed effort, however, any such agreement must not come at the expense of protection for personal data

and freedom of information for individuals. An appropriate balance must be found for the various legal positions.

5.3 Cloud computing: Sunny with a chance of rain

Cloud computing has evolved into a widespread business model – reason enough for me to examine this issue carefully at national and international level.

In just a few years, cloud computing has gone from being a technological trend with a limited number of services to a business model firmly established in the global marketplace. The cloud is everywhere, used for everything from accessing stored e-mails, photos or music from smartphones to running complex IT processes. Much of the time we are not even aware that we are using cloud services, where the data are stored or where they are being processed. Using the cloud cannot only simplify data processing and lead to lower costs; under certain conditions it can also produce additional synergies and increase IT security.

I have already reported at length (23rd Report, no. 5.6) on the risks to the storage and processing of data in globally networked data centres associated with the often-used model of data processing of other bodies on behalf of the controller under the European Data Protection Directive and Section 11 of the Federal Data Protection Act (*Bundesdatenschutzgesetz* (BDSG)). The Article 29 Working Party adopted respective Binding Corporate Rules (“BCR for processors”), a significant development during the reporting period (see no. 2.4.1.2).

In this context, however, the possibility of access for government agencies, especially those from third countries, to data stored in the cloud remains problematic. This problem affects providers of cloud services which are subject to legislation such as the US Patriot Act, for example, and could thus be required to disclose data to foreign security authorities. Even sub-contractors of US companies which are located within Europe but store data outside the US may be affected. This assessment was recently confirmed by a study conducted by the Institute for Information Law at the University of Amsterdam (http://www.ivir.nl/index-english.html).

This is one reason I believe it is necessary for the controller alone to securely encrypt personal (in particular sensitive) data according to the state of the art before uploading and storing them in the cloud.

The lack of legal certainty for processing outside the EU/EEA and the high level of data protection within the EU, however, could create a competitive advantage for cloud “Made in Germany” or Europe.

The IT security industry and data protection commissioners are intensely studying this issue (see also box for no. 5.3). But many questions remain.

For example, creating a general legal framework for data protection certification and a seal of quality as in the case of De-Mail in Germany is conceivable (see no. 3.2.4). International norms and standards could ensure global comparability of secure cloud solutions that provide the necessary data protection. Other developments, such as the expected EU General Data Protection Regulation (see no. 2.1.1) are also likely to bring changes to cloud computing.

So it will be interesting to see what the future holds.

Box for no. 5.3

Working groups and publications on cloud computing

The 82nd Conference of Data Protection Commissioners of the Federation and the *Länder* adopted a guide to cloud computing which is aimed at decision-makers, private- and public-sector data protection officers and those responsible for IT and is intended to promote the use of this technology in line with data protection principles. http://www.datenschutz.bund.de

The Article 29 Data Protection Working Party published the Working Paper 196 of the European Data Protection Commissioners in July 2012. This paper draws attention to legal problems and risks associated with cloud computing and offers helpful information. The paper mainly focuses on applicable law for the obligations and responsibilities of cloud providers and cloud users, technical and organizational measures to protect data in the cloud, and legal and technical instructions for data transfers to third countries. In particular, the paper notes that all sub-contractors should be named and all relevant details should be disclosed and dealt with in a contract. The opinion also includes technical and organizational measures of data

protection and data security like those published by the conference of data protection commissioners of the Federation and of the Länder in its paper on modern data protection law for the 21st century (“Ein modernes Datenschutzrecht für das 21. Jahrhundert”). According to this are listed confidentiality, integrity and availability as well as isolation (unlinkability in the sense of the German term “Unverkettbarkeit”), intervenability, accountability and portability as core security objectives. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf#h2-1

Additional discussions at international level took place in the International Working Group on Data Protection in Telecommunications (IWGDPT) in spring 2012 and at the 34th International Data Protection Conference in Uruguay last autumn (see no. 2.4.3). In its Sopot Memorandum, the IWGDPT refers to the urgent need for greater transparency, while a resolution adopted at the International Data Protection Conference focused on reviewing and enforcing an adequate level of data protection as well as paying attention to and implementing privacy by design (PbD) at an early stage of development. http://datenschutz-berlin.de/content/nachrichten/datenschutznachrichten/%2027-april-2012, http://www.datenschutz.bund.de

The Federal Commissioner also was involved in the Working Group on a Legal Framework (AG-Rechtsrahmen) of the Federal Ministry of Economics’ Trusted Cloud Initiative (www.trusted-cloud.de) and in several working groups of the Federal Government’s IT Summit Working Group 4 (AG 4). Papers related to data protection were drafted in both areas. The Working Group on a Legal Framework has published a ten-point policy paper (“Datenschutzrechtliche Lösungen für Cloud Computing - Ein rechtspolitisches Thesenpapier”) addressing problems in cloud computing related to data processing on behalf of others, the issuing of certificates and possible accreditations. A document on legal requirements for secure cloud services drafted in the IT Summit sub-group on cloud computing has unfortunately not yet been published. At a meeting of AG 4 in Bonn in September 2012, it was clear that cloud computing is a controversial topic within the IT industry and that IT security and data protection issues remain unresolved, even though cloud services, when their use is ordered in contract form, do not differ “all that much” from classic IT outsourcing in terms of data protection law, other than that data are stored and processed at unknown locations.

In general, standards and certification for cloud computing are currently being demanded. As a first step, the Federal Office for Information Security (*Bundesamt für die Sicherheit in der Informationstechnik* (BSI)) drafted and published a policy paper, with my input, containing basic requirements, requirements for a high level of both confidentiality and availability, based on baseline security for IT systems when using cloud computing, and information about data protection. This paper can be accessed at www.bsi.de. As a second step, IT security certification for cloud technologies is currently being prepared. Germany will soon have tested IT security for cloud computing.

5.4 At an impasse: The cookie rule

It is not clear whether and on what legal basis the provision of the E-Privacy Directive known as "the cookie rule" is to be applied.

The matter is at an impasse: The responsible Federal Ministry of Economics and Technology still believes that the Telemedia Act (*Telemediengesetz* (TMG)) has always governed the need for consent to use cookies (see 23rd Report, no. 4.4); the data protection supervisory authorities continue to apply the provision concerning the right to object in Section 15 (3) of the Telemedia Act; and the European Commission remains silent. It is reviewing the matter.

Providers of Internet services who want to comply with the law and users who do not want to be monitored secretly are both unsure. Both providers and users are continually asking the data protection authorities for a solution.

What could a possible solution be? An attempt by the SPD parliamentary group in January 2012 (Bundestag document 17/8454) to lock in the consent solution by amending the Telemedia Act was unsuccessful, as were my efforts during deliberations on the amendment of the Telecommunications Act (*Telekommunikationsgesetz*, TKG) (see no. 6.4). Should we fall in with the ministry's position? Directly apply the Directive because it has not been implemented? Wait for a signal from the Commission? An ideal solution seems to be impossible. Perhaps we will have to wait for a court ruling to show the way.

Initial technical solutions for consent are already being used or developed. Because ambiguities remain here, too, the Article 29 Working Party has started gathering and

assessing various solutions in order to achieve uniform implementation of the cookie provision. It is also guided by its “Opinion 4/2012 on Cookie Consent Exemption” (WP 194). The results will be published in due course.

There are efforts at international level to develop a “Do-not-track-standard” (DNT) which would enable users to make a binding declaration on tracking their visits to websites; this would also cover the placement of cookies. The DNT standard that the W3C (World Wide Web Consortium) is working on was originally supposed to be published in early 2013. But the work is taking longer than planned, also due to conflicting interests and goals within the W3C task force.

The Article 29 Working Party therefore has major doubts whether the standard (at least in the “soft” form preferred by most of the representatives in the W3C who are close to business will in fact meet the requirements of Article 5 (3) of the E-Privacy Directive. To comply with European law, a solution would have to make “do not track” a binding header command and would not only prevent advertising, but even the placing of cookies and the collection of data for advertising purposes. And this must apply to all providers, whether they are providers of the website visited (first party) or advertising providers (third party).

5.5 Behind closed doors: ICANN and its new contracts with registrars

It has largely escaped notice that the contracts between ICANN and registrars are being revised and expanded to include additional obligations, unfortunately also at the expense of data protection.

Few Internet users know what ICANN is or what it does. In short, the Internet Corporation for Assigned Names and Numbers is a non-profit organization located in the US that coordinates the assignment of names and addresses on the Internet. Registrars in the various countries, often Internet service providers, are as final links responsible at local level for assigning domain names and distributing IP addresses to persons and organizations. To this end, ICANN makes contracts with the registrars which govern what end-user data must be collected, stored and published in the WhoIs databases.

These contracts are currently being revised. In addition to the registrars, other participants in this process are representatives of law enforcement authorities and, in a purely advisory capacity, the GAC (Governmental Advisory Committee), which has

a permanent seat at the European Commission. Advocates of data protection do not have a voice.

So it is not surprising that the wishes of the law enforcement authorities in particular have been granted and are to be included into the new contracts: annual re-verification of registrants' contact data (e-mail address, telephone number), to be published in the WhoIs database; and storage of far more personal data than is needed for commercial purposes, such as additional banking information, IP addresses, log files, etc. These data are intended to make the work of law enforcement authorities easier and enable them at least to solve Internet crimes, if not prevent them.

ICANN has long been aware of one of the main reasons for so much false information in the WhoIs database: Accurate contact information, especially of private individuals, is used by spammers, so registrants provide false information for their own protection. Introducing the OpoC model (Operational Point of Contact) could help, but this has not yet happened. Queries from authorized bodies would then be answered by a trustworthy body administering the WhoIs data. This model would replace the public WhoIs databases and thus serve the interests of private persons in protecting their data.

In September 2012, the Article 29 Working Party wrote to ICANN to object to the additions to the contracts, saying that they were in violation of European law: Registrars may not collect and store data for law enforcement purposes as a precaution and without a legal basis when these data are not necessary for contract-related purposes or for providing the service. If ICANN obligated them to do so by the terms of its contracts, they would violate European law.

It is not clear whether a compromise can be found or an exception be made for EU registrars, as ICANN referred to in its response. The negotiations are still under way.

5.6 IPv6: Do good things really take this much time?

There are two sides to the brave new world of new number plate requirements for the data autobahn: "Paranoid" users are first of all struck by the immense potential for surveillance and the ability to identify individuals. But the reorganization of IP addresses also offers room for data protection-friendly solutions and thus ultimately for "safe driving" on the data autobahn.

Technologies and trends on and related to the Internet typically spread and evolve rapidly, much faster than we were used to in other areas. But even when it comes to the Internet, there are exceptions that prove the rule. Only a few years after the current Version four of the Internet protocol (IPv4) was introduced in 1983, it was clear that, with the dramatic expansion in the number of users, the supply of available addresses would soon be exhausted. But in 1998, when the subsequent protocol started to be standardized, one would certainly have been surprised to know that the last block of addresses in Europe would not be issued until early 2012.

Compared to IPv4, the succeeding Internet Protocol Version six (IPv6) increases the availability of addresses by the incredible factor of 2 to the 96th power, offering a total of around 340 sextillion addresses. This means that every square metre of the earth's surface could contain about 655,570,793,348,866,943,898,599 addresses. If every IP address were the size of a grain of sand, the total number of IPv4 addresses would form a ball eight centimetres in diameter, while the total number of IPv6 addresses would form a respectably sized asteroid with a diameter of 350 kilometres. Unlike its predecessor, an IPv6 address is divided into two parts of equal size (each 64 bits). The front part, known as the *prefix*, is largely used to identify the network segment, for example the specific house connection. The rear part, the *interface identifier*, is completing the address and is the identification of the individual network card (see Box a for no. 5.6).

It has long been known that the number of Internet addresses available under IPv4 was growing scarce. Nonetheless, the "sudden" realization that the last address blocks were being assigned in early 2012 led to some panic in companies and public authorities and to an increased push to use the no longer very new protocol IPv6. The problem with this is that the expansion of the address space goes along with a fundamentally new strategy for assigning addresses. It will (on principle) be possible in the future for every device connected to the Internet to have its own permanent address – practically a number plate for every computer, coffee-maker and electricity meter. Those whose businesses are based on registering user behaviour and creating user profiles would be eager to get their hands on this information.

But until now this has remained in the realm of theory, as it was very difficult to get the protocol for one's own Internet connection. This product only became available when it was quietly introduced by a major provider that does not view IPv6 as a new product, but as a technical advance in existing products. Since September 2012, every new customer who applies for Internet access with this provider receives an

IPv6-based connection, although most customers are probably not even aware of it. Since then, immediately re-issuing prefixes when disconnecting and rebuilding connections took priority and was also carried out. So far, however, the lack of a forced disconnection means that amateurs of changing addresses must set up a new prefix either manually by disconnecting or semi-automatically by setting a timer for the router's power supply. But more convenient solutions can be expected soon: a button at the configuration interface to force a new prefix, and a function that does this automatically at certain intervals.

According to the results of my survey in 2011, nearly one-third of the 33 providers of Internet connections surveyed during the reporting period were not planning to introduce IPv6. The remaining two-thirds said that they were planning to assign prefixes to end users dynamically. I am pleased to note that this is in fact happening, as demonstrated by the quickest in industry.

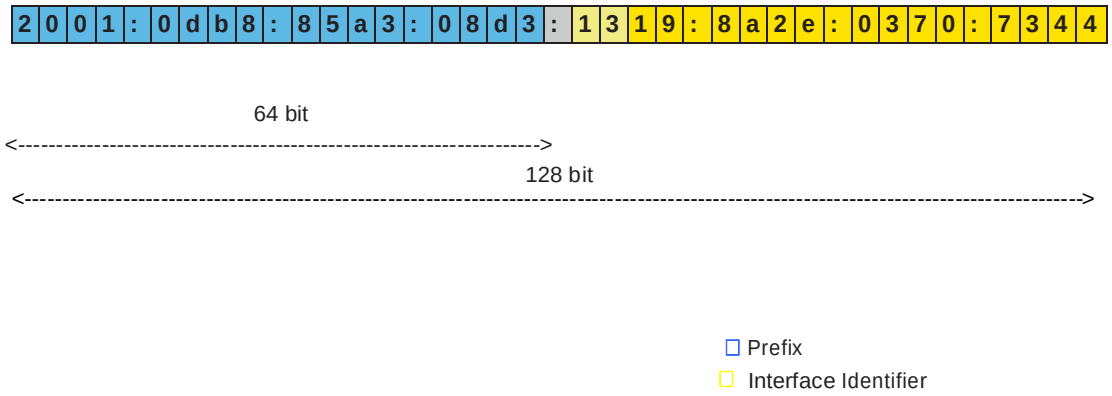
The transition to the "new" protocol has been discussed in various national and international bodies with regard to data protection-friendly introduction and design (see box b for no. 5.6).

In addition, the task force on technical and organizational data protection issues of the Conference of Data Protection Commissioners of the Federation and of the *Länder* has elaborated a guide to "Data Protection with IPv6" for manufacturers and providers of services to retail customers. This guide addresses the most important issues related to the transition.

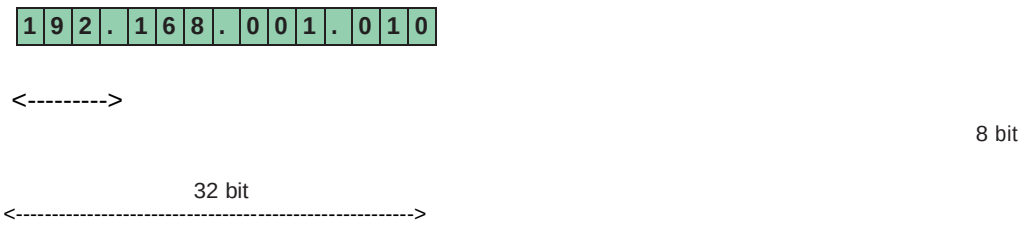
To illuminate the effects the transition to the new Internet protocol will have, in November 2011 I organized a symposium on IPv6 in Berlin. I was especially interested in establishing a broad interdisciplinary discussion forum and taking advantage of the resulting synergies. The invited speakers, from private industry and the research community, provided for transparency in their presentations and contributions to the discussion and explained the advantages and disadvantages of a gradual transition to the new protocol. The presentations and discussions were documented in the form of conference proceedings, which can be accessed from my website (www.datenschutz.bund.de).

Box a for no. 5.6

Structure of an IPv6 address



Structure of an IPv4 address



Box b for no. 5. 6

Box b for no. 5.6

The 82nd and 84th National and the 33rd International Conference of Data Protection and Privacy Commissioners all addressed the issue of IPv6 and identified the following requirements:

– Providers should, on principle, assign dynamic prefixes to customers free of charge; they should assign a static prefix only at the customer’s special request.
– If it is not possible to assign a dynamic prefix, customers must be given the opportunity to change the prefix.
– Interface identifier and prefix should be changed synchronously.
– Interface identifiers should be scrambled by default (“privacy extensions”).
– Parts of the address that are not needed to measure online audiences should be deleted (only the first 4 bytes are necessary).

– Running IPv6 and IPv4 together (“Dual-stack operation”) should be avoided; this also applies to the tunnel protocols used as an interim solution.

The resolutions are available at www.datenschutz.bund.de.

5.7 Websites of federal authorities

Citizens must be confident that their data are protected also when communicating with public authorities electronically. Unfortunately, I found that this was not always the case.

There are many websites that citizens can use to easily communicate with public authorities, for instance to request information material or to ask questions. To do this, they have to enter personal data in the embedded contact forms. Although transmission of these data are to be encrypted in line with Section 9 of the Federal Data Protection Act, this was not always the case.

In November 2010 a petitioner wrote that the website of the Federal Anti-Discrimination Office (*Antidiskriminierungsstelle des Bundes*) did not meet applicable data protection provisions. Personal data such as name, address and e-mail address entered in the contact form on the office’s website were transmitted without encryption. This led me to randomly check other federal authorities, and I discovered similar cases. They violate the annex to Section 9 of the Federal Data Protection Act that requires providers “to ensure that personal data cannot be read, copied, altered [...] without authorisation during electronic transfer or transport”.

In January 2011 I asked the data protection officers of the supreme federal authorities to examine all websites of their own and of their executive agencies. By March 2011 the 43 commissioners I contacted named 77 websites run by federal authorities.

According to this feedback 22 websites used encrypted and 34 unencrypted contact forms. However, seven agencies using unencrypted forms were preparing appropriate encryption. Twenty websites did not use contact forms at all. As another positive effect, my request prompted several agencies to encrypt their contact forms, and one unencrypted form was immediately deleted. In April 2011 I informed the data protection officers of the supreme federal authorities about the result of my survey

and asked them to establish immediately encryption for all forms yet unencrypted. According to my knowledge, all agencies have completed this procedure.

In addition to the letter mentioned above, I reminded the federal agencies in January 2011 that using the Facebook “Like button” on their websites is not acceptable from the data protection point of view. At that time, federal agencies did not use the Facebook Like button on their websites; only one federal agency planned to embed this social plug-in (see no. 5.8.3).

I will continue to check whether the federal agencies’ websites fulfil data protection standards in the future. However, facing the bulk of websites and their regular adaptations and extensions, unfortunately I will not be able to ensure comprehensive and up-to-date supervision.

5.8 Social networks

The number of users and the significance of interactive online services have increased also during the present reporting period. In this context, social networks stand out by both their huge number of users and the way they are used. While private users enjoy the possibilities to stay in touch with “friends” (including real friends but also distant acquaintances), commercial and administrative users find new ways to address customers or citizens. However, these new opportunities come at the cost of data protection risks. Reason enough to scrutinize such services further on and insist on solutions that meet data protection needs.

Facebook is the most successful social network, and perhaps also the most popular one. A look into the processing of user data was to show whether the millions of users have made the right choice – from a data protection perspective. All European data protection authorities were equally interested in such an audit as more and more “coups” kept being revealed. The audit was carried out by the Irish data protection authority.

5.8.1 Everything ok? Facebook after the audit

The Irish data protection authority examined the social network Facebook and published the results in a report. Nevertheless, many data protection issues remain unresolved.

Some might wonder why the Irish data protection authority should examine a US social network and is even supported by that network; and why German data protection authorities could not do the same thing. The answer is both simple and inexhaustive: Facebook Ireland Ltd. being the responsible body for data processing in Europe, data processing as such is carried out on their behalf by Facebook Inc. in the USA. Says Facebook Inc.

If we accept this construct, the Irish data protection law applies in line with the EU Data Protection Directive 95/46/EC and the Federal Data Protection Act so that the Irish data protection authority is responsible for supervision. However, it does not claim sole responsibility. This is one reason why European data protection authorities were able to discuss the problems they have in their respective countries in the Article 29 Working Party and ask the Irish data protection commissioner to take them into consideration.

Some of Germany's state (Länder) supervisory authorities do not share Facebook's position; they consider themselves responsible, too, because data of Facebook users are collected and used in Germany. However, Facebook insists on its position with the result that demands according to German data protection legislation had not been taken into consideration where there are no comparable provisions in Irish law.

For example, this applies to Facebook's real name policy which Facebook stated in its terms of use. Reason: The idea behind the social network is that people know whom they are dealing with. And: Security must be ensured. However, Germany's Telemedia Act requires providers to enable consumers to remain anonymous or to use pseudonyms as far as technically possible and reasonable. Since the Irish data protection law lacks such a provision, no objections were raised against the real name policy. The EU General Data Protection Regulation is intended to create greater harmonization and thus solve these and similar problems caused by globalized information processing and different or missing national laws (see no. 2.1).

To enforce its "name directive", Facebook encouraged users to report users registered with a false name. As a result, Facebook will lock the account of the reported user until the person concerned discloses his/her (real) identity by submitting a copy of his/her ID card. This "crackdown" prompted a German supervisory authority to issue an order against Facebook requiring the company to allow pseudonyms and restore locked accounts. The proceedings had not yet been completed at the time this report went to press.

Discussions with Facebook might result in a compromise proposed by the Article 29 Working Party in its opinion on online social networking (WP 163) as a privacy-friendly solution: Users must provide their real data when registering for the network but may act under a pseudonym within the network.

In December 2011 the Irish data protection authority published the report on the audit carried out in line with Irish and EU law over several months. Facebook was invited to comment on the report and to amend and update its policy. The Irish data protection authority examined these measures and published its final report in September 2012.

Overall, users benefited from the audit. For example, Facebook's terms of use and its directives on data use became more transparent by providing more clarity and detail, and users have more control over their settings and better access to their data. A great success was that facial recognition has been disabled for all users in the EU. Credit for this goes not only to the Irish data protection authority, but also to the commitment of German supervisory authorities.

In addition to the real name issue, there is the demand for privacy by default. Though not a legal requirement, the Article 29 Working Party also considers privacy by default a key element of exemplary data protection policy that should be implemented for the users' benefit. The Irish data protection authority will advocate this position during further consultations with Facebook. Unfortunately, Facebook (among others) finds it difficult to accept this. So, not everything ok (yet)?

5.8.2 May public authorities use Facebook fanpages?

Agencies frequently ask me whether they are allowed to use fanpages. However, a definite answer is not possible.

Many private companies are using fanpages on Facebook to present new products and to promote their business, for example. In the reporting period, great public interest was shown in pages used by the police to search for wanted or missing persons (see no. 7.4.7). The responsible ones concerned seem to consider Facebook an appropriate channel to reach a young audience and interactively communicate with users. Federal authorities are also exploring the new possibilities,

running their own pages or planning to do so. While I understand the aim of reaching a specific audience through fanpages, data protection must be observed.

A fanpage is a kind of website published (“hosted”) by Facebook. However, responsibility for content posted on the fanpage lies with its owner, i.e. the individual agency, and not Facebook. Potential fanpage owners must first register a new user account before setting up and maintaining a page. The registered person or body is thus both a Facebook user and, by running a fanpage, a service provider within the meaning of the Telemedia Act.

When examining whether using fanpages is permissible it is important to note that although Facebook is a US business, the European market is served by Facebook Ireland Limited. Therefore, the Irish data protection commissioner is responsible for supervising data protection. In an audit and re-audit he examined whether Facebook meets data protection standards and asks Facebook to implement such standards, where necessary (see no. 5.8.1). Although in the course of this audit Facebook significantly improved its data protection policy and promised to implement further data protection standards, I am still concerned about certain issues such as the transfer of user data to the USA. As soon as Facebook has implemented its new data protection policy I will examine whether and under what conditions it would be acceptable from a data protection perspective for federal authorities to set up fanpages.

Regardless of whether pages are permitted, services offered by agencies in social networks must be in line with data protection law. This means, for example, that federal agencies or health insurance funds must not invite users to disclose sensitive information via the fanpage on the social network. Some problems may be avoided by redirecting users from the fanpage directly to a website hosted by the agency. In any case, agencies should communicate with citizens via secure channels such as ssl-encrypted forms or via De-Mail (see no. 3.2.4). They should avoid sending “private messages” via a system which is technically operated outside Europe, whenever possible.

5.8.3 Integration of social plug-ins meeting data protection requirements

Nowadays, many websites use so-called social plug-ins, one of the most popular being the “Facebook Like button”. Using this button without special precautions

violates data protection law. Technically, such issues can be mitigated by applying a "two-click procedure", for example.

By integrating plug-ins of popular social networks website operators hope to increase the number of visitors, because websites are recommended in these networks. Federal authorities are also trying to reach a larger audience by integrating social plug-ins. As the example of the Facebook Like button shows, such attempts should be looked at with a critical eye as regards data protection.

When adding the Like button, Facebook embeds a Facebook frame in the website's source code. Every time a user opens the website, a Facebook cookie will be placed that is valid for two years. In addition, the referer (address of the website from which the user was redirected to the current website by clicking on a link) and the corresponding URL are transmitted to the Facebook server each time the website is visited. That way, the service provider can see which website a user has just visited, and users may be tracked by persons who are not even Facebook members. If the website is visited by a logged-in Facebook member, the script also transmits the session ID to Facebook that directly can identify the person concerned. This helps the business record the persons' Internet use by their names and create profiles.

This kind of data transfer violates Section 13 (1) of the Telemedia Act (see box for no. 5.8.3).

In November 2011, a German publishing house presented the two-click solution for an integration of social plug-ins meeting data protection requirements. With this approach, social plug-ins are disabled when opening the website so that no data are transferred. However, the plug-ins may be activated by clicking on them. When doing this, users will in the first instance be informed in line with the Telemedia Act that personal data will be transferred to the social network and might be stored in non-European countries. This allows users to decide themselves whether they want this or not. Only then will the embedded programme be activated as described above. In my view, this is a feasible approach to integrate social plug-ins in websites while meeting data protection requirements.

Box for no. 5.8.3

Section 13 (1) of the Telemedia Act

Obligations of the service provider

The service provider must inform the recipient of the service at the beginning of the session about the nature, scope and purpose of the collection and use of personal data and about the processing of his data in countries outside the scope of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ EC No. L 281 p. 31) in generally understandable form, unless such information has already been provided. In the case of an automated procedure which permits subsequent identification of the recipient of the service and prepares the collection or use of personal data, the recipient of the service must be informed at the beginning of this procedure. The content of this information must be accessible by the recipient of the service at any time.

5.9 Battling giants

The French CNIL completed its examination of Google's new privacy policy, which was a pilot project "one for all" pilot project of the Article 29 Working Party. Now preparations have started to examine Microsoft's terms of use and the privacy statement as well.

In January 2012, Google announced that it would introduce a new privacy policy on 1 March 2012. This policy would be fully revised and improved for the benefit of users: It would be simple, clear and transparent. When the Article 29 Working Party suggested postponing the date to allow for checking compliance with data protection law, Google refused. The explanation was surprising: Users had had more than one month to read and understand the new Privacy Policy. Google was confident that European data protection requirements were met.

However, key points of the published privacy policy did not meet EU data protection requirements at all. This was already the result after an initial analysis carried out by the French data protection authority (CNIL), as central coordinator on behalf of the Article 29 Working Party, immediately after the privacy policy was published. While merging the numerous (70!) policies in one fairly well-structured document understandable by a normal Internet user may be considered an improvement, accuracy and detail were lost and replaced by general statements such as:

“We may probably collect device-specific information (such as your hardware model, operating system version, unique device identifiers and mobile network information, including your phone number). Google may associate your device identifiers or phone number with your Google Account, if applicable.”

“We also use this information to offer you tailored content – such as giving you more relevant search results and ads.”

Such wording leaves much room for arbitrary interpretations, certainly for the benefit of Google. It leaves users at a loss and with no more information than before.

Users are not sufficiently informed, neither about the purpose of a specific service they want to use nor about the required data and access rights. A more serious, because more intrusive and incalculable, problem is that Google links and analyses user data from various services that Google introduces without further ado: there is no provision of more details and in particular no consent - or at least a right to object. In this way, not only can Google create detailed user profiles, it can also use these profiles from different services to create meta-profiles. Google CEO Larry Page explains that innovative services with an additional value for users can be developed only when linking data. Is this a silent reproach that data protection commissioners slow down technical progress by excessive regulation and restrictions? Such allegations are being made also by other stakeholders in the discussion about the ambitious European data protection reform (see no. 2.1).

As soon as the Privacy Policy went into effect, CNIL started its detailed examination of compliance with data protection law. What followed was a game of questions and answers with Google formally showing its will to cooperate but actually trying to evade key questions. The European data protection commissioners of the Article 29 Working Party were closely involved in the process.

Google was informed of the results in October 2012. In sum, Google does not comply with the key principles of data protection, in particular purpose limitation, data minimization, proportionality and the right to object. Google was given time to revise its privacy policy and to make the required practical changes by February 2013. Although Google said it was willing to cooperate, previous experience suggests that Google will seek to delay the process by continuing correspondence and presenting new arguments. The Article 29 Working Party will be prepared for this and respond accordingly.

In September 2012 Microsoft modified its Services Agreement and announced further revision. The Article 29 Working Party decided to conduct an audit similar to that for Google, because these changes also affect the Privacy Policy and numerous Microsoft services. The audit will be headed by the data protection commissioner of Luxembourg (CNPD), assisted by CNIL. Microsoft was informed of the planned audit in December 2012 and asked to postpone its revision until the audit is completed.

5.10 The bill please!

Apps have taken over what used to be done by diallers. But customers are still the ones to pay.

They are so cute and even useful, these free apps for our indispensable companions, the smartphones. They help you keep your kids entertained or adjust a shelf. The annoying part is when you – for lack of a third hand – tap the banner ad instead of the buttons of your level app. In such a case it might have been cheaper to buy a real tool.

Petitioners told me that many ads in free smartphone applications use insidious practices to rip off customers. The petitions convinced me to have a closer look at this issue.

Reserving ad space in apps is a standard procedure of the industry to cover part of the development costs. Usually advertising networks fill the ad space with content which developers cannot influence. With this strategy both the provider of the ad space and the advertiser want to make profit from customers. Tapping on a banner ad often will redirect you to a so-called landing page, a webpage specially designed to inform you about the offer shown in the banner ad. However, it is not important which page you open, but which (invisible) information is transferred.

Telecommunications operators told me that media service providers frequently receive the Mobile Subscriber ISDN Number (MSISDN), which is the customer's worldwide unique telephone number, so that they can charge for their services via the telephone company. This has been going on for more than ten years. Customers are informed about it when signing the contract – data are transferred only to contract media service providers. However, the renaissance of a protocol, the Wireless

Application Protocol (WAP), thought to have disappeared a long time ago, is surprising in this context. The predecessor of today's "mobile Internet" has never been widely used and finally sank into oblivion (for the time being). This protocol has always transferred data such as the MSISDN as a convenient way to purchase services. But because it now operates silently in the background, many customers are not aware of the fact that they made a purchase by just tapping a banner; whether this always really concludes a contract is questionable, to say the least.

Moreover, modern Internet protocols do not seem entirely free of this industry either. Reports suggest that such personal data are also transferred within the protocol header via or using the Hypertext Transfer Protocol (HTTP). I have earmarked this issue for the next reporting period so that I can form my own opinion of the technologies and procedures.

In addition to the procedures, the legal basis for transferring personal data must be discussed in this context. The Federal Network Agency (Bundesnetzagentur) took on the topic and launched a survey among the providers concerned in 2011. Although final results are not yet available, the present situation is as follows: Section 97 (5) of the Telecommunications Act (see box for no. 5.10) does not apply to the transfer of MSISDN, because the business model is based on factoring, i.e. the company bills its own claims, not those of a third party. According to the Bundesnetzagentur, users must always agree to data transmission. Without their consent, the transmission would have no legal basis and thus be inadmissible.

Box for no. 5.10

Section 97 of the Telecommunications Act (extract)
Charging and Billing

(5) Where the bill from the service provider includes payment for third-party services supplied in connection with the provision of telecommunications services, the service provider may transmit to the third party customer data and traffic data to the extent that these are required in a given instance to enforce third-party claims in relation to the subscriber.

6 Telecommunications and postal services

6.1 Preventive data retention: A never-ending story?

For more than six years now, opinions have been divided over data retention for the purpose of preventing crime. The concerns of various European courts must not be ignored. But the "what" and "how" of new regulations remain unclear.

In my last report, I asked: "Preventive data retention: Quo vadis?" (see 23rd Report, no. 6.1). Despite extensive discussion, two years later it is not clear which direction European and German legislators will take.

For example, in April 2011 the European Commission published an Evaluation Report on the Data Retention Directive (2006/24/EC) listing a whole series of shortcomings in almost every area covered by the directive. For example, the goal of harmonizing the European telecommunications market was apparently not achieved. The report also criticized the fact that informative statistics needed for a comprehensive assessment of the directive's implementation in the member states were poor, that they were not telling very much and, in some cases, even were not made available by member states. The report also found various shortcomings, for example in definitions or purpose limitation requirements for data use. Lastly, it is clear that the maximum retention period allowed by the directive of two years is much too long: 70% of the data requested by the security authorities was no more than three months old and only 10% was older than six months.

In view of these obvious and significant problems, I was surprised by the European Commission's statement that the directive had proved valuable overall and only needed some revising. Over the course of 2011, several workshops to discuss special solutions were held with representatives of industry, governments, non-governmental organizations and data protection supervisory authorities. The Commission also requested several studies, including one on the possibility of data preservation ("quick freeze") in connection with preventive data retention. However, no results have been presented yet, whereas the date for publishing the draft of a revised directive has been repeatedly postponed. The draft was initially supposed to be ready by late 2011, but in October 2012 Commissioner Malmström announced that she could not yet say when it would be ready. She mentioned the technical and legal complexity of the issue, among other things, as reasons for the delay. It seems strange that the Commission, which itself is unable to revise a directive which is rated inadequate, is at the same time insisting that member states transpose the directive into national law. Germany's first attempt at implementing the directive into national

law was struck down by the Federal Constitutional Court (*Bundesverfassungsgericht*) in spring 2010. Its subsequent attempts to pass legislation were taking too long for the Commission, which in May 2012 brought legal proceedings against the Federal Republic in the European Court of Justice for failing to implement the directive.

Although the Federal Ministry of Justice took up my proposal and in July 2011 presented an initial draft for discussion of "quick-freeze" legislation (Act to preserve existing traffic data and to guarantee access to inventory data on the Internet (*Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet*)), this draft has not made it to the Cabinet, because the Federal Ministry of the Interior continues to insist on comprehensive preventive data retention. The draft was intended to create a legal basis for law enforcement authorities to order telecommunications companies to temporarily save data of a specific customer suspected of wrongdoing. In order to "freeze" traffic data which are stored for commercial purposes only briefly or not at all, the law in addition provides for a limited data retention order for certain categories of data such as dynamic IP addresses. This approach makes the comprehensive retention of traffic data without a reasonable suspicion of wrongdoing unnecessary, especially since such data are typically stored for several months anyway for commercial purposes and are thus generally available for law enforcement purposes (see no. 6.7). I still believe this procedure to be a valid alternative to the comprehensive and reasonless preventive retention of all data and that it both serves the public interest in prosecuting crimes, on the one hand, and protects the confidentiality of telecommunications and the right to informational self-determination on the other, to a degree acceptable to both sides.

The re-introduction of blanket preventive data retention does not seem useful also because even after four years, there is no evidence that it is needed at national or European level. A study by the Max Planck Institute published in January 2012 even came to the conclusion that stopping preventive data retention in Germany as a result of the Federal Constitutional Court decision of 2 March 2010 had no serious impact on law enforcement effectiveness. But perhaps the fate of preventive data retention is not in the hands of the Commission or national legislators at all. Following the Irish High Court, Austria's Constitutional Court in 2012 asked the European Court of Justice for a preliminary ruling to review whether the Data Retention Directive complies with the EU Charter of Fundamental Rights. I believe it is certainly possible that the court's review will find that the directive fails at least in part to comply with the European fundamental rights. Whether this ruling will finally put an end to

preventive data retention or is merely the beginning of a new chapter remains to be seen.

6.2 Of double doors and IP addresses: The Federal Constitutional Court ruling on providing information about inventory data

The Federal Constitutional Court ensured greater clarity on the need to protect IP addresses and created the need for legislative action.

On 24 January 2012, the Federal Constitutional Court came to a ruling on the constitutionality of Sections 111 through 113 of the Telecommunications Act (*Telekommunikationsgesetz* (TKG)). The highest court's decision on the legal classification of requests for information on subscribers using dynamic IP addresses and the introduction of the so-called "double-door" principle have proved to be milestones of data protection in telecommunications law.

The ruling (1 BvR 1299/05) came in response to a constitutional complaint lodged in 2005 concerning the provisions of the Telecommunications Act on the procedure for requesting information about inventory data. According to the applicants, both the procedure for collecting data for purposes of responding to requests for inventory data (Section 111 of the Act) and the procedures for the automated (Section 112) and manual (Section 113) provision of information violated the privacy of telecommunications and the right to informational self-determination.

The court only partly agreed. It found Sections 111 and 112 of the Act in compliance with Germany's constitution, the Basic Law (*Grundgesetz*), and only objected to Section 113 (see the court's headnotes in the box for no. 6.2). The court found that Section 113 (1) second sentence of the Act violated the right to informational self-determination by allowing the security authorities to retrieve data used to secure access (in the form of passwords, PINs or PUKs) to devices and storage systems such as mobile telephones and e-mail accounts, whether or not the authorities met the conditions for using these access codes.

The court dealt with two other issues which are crucial from the perspective of data protection law. Firstly, the court made it clear that requests for telecommunications data must always include an authorization for the provider to transfer the data and a legal basis for the authorities to request the data. According to the court, which called it the "double-door" principle, this means that before a telecommunications services

provider can hand over data to the authorities, the provider and the authorities each need a legal basis, a door they must go through, before the data can be transferred. Specifically, the court clarified that Sections 112 and 113 of the Telecommunications Act represent only the authorization for the provider to transfer the data and not the legal basis for the authorities to request the data. A legal basis for the latter must be created in the particular statutes of the authorities requesting the data. The court found that for the procedure given in Section 112 of the Act it was sufficient to have provisions generally authorizing the collection of personal data, but that for the manual procedure a special legal basis was needed to clearly authorize the retrieval of data under Section 113 of the Act.

Secondly, the court made its first clear pronouncement on the nature of information on the inventory data of subscribers using dynamic IP addresses, ending a debate that had gone on for years (see 22nd Report, no. 7.11). The court made clear that, in its present form, Section 113 of the Telecommunications Act cannot serve as the legal basis for the relevant right of access, stating that an explicit and clear legal authorization was needed for this purpose and that such authorization did not yet exist. What I find especially positive is the court's finding that, to identify dynamic IP addresses, telecommunications companies would first, by making an interim step, have to look through their customers' traffic data and thus draw on specific communications transactions which are protected by Article 10 (1) of the Basic Law on the privacy of telecommunications. Wherever access to data guaranteed the privacy of telecommunications is imperatively necessary in response to requests for information, however, the court found that the protection given by Article 10 (1) of the Basic Law extended to the entire process of requesting information.

The court gave legislators until 30 June 2013 to amend the Act in light of the court's decision. The amendment process has already been initiated (see no. 6.3). In any case, with this decision the Federal Constitutional Court has once again reinforced data protection in the field of telecommunications.

Box for no. 6.2

Headnotes of the Federal Constitutional Court ruling on requests for information about inventory data

1. Identifying the telecommunications numbers of subscribers constitutes an intrusion into the right of informational self-determination. On the other hand, identifying dynamic IP addresses constitutes an infringement of Article 10 (1) of the Basic Law.

2. When establishing a process for requesting information, legislators must create a legal basis for both the retrieval and transfer of data.

3. The automated retrieval of information under Sections 112 and 111 of the Telecommunications Act complies with the Constitution. Section 112 of the Act requires separate bases for authorizing retrieval.

4. The manual retrieval of information under Section 113 (1) first sentence, Section 111 and Section 95 (1) of the Telecommunications Act complies with the Basic Law when interpreted in accordance with the Constitution. Firstly, in order to retrieve data qualified legal bases are required which obligate telecommunications companies to provide information in a clear manner. Secondly, the provision many not be applied to identifying dynamic IP addresses.

5. The security authorities may request information about access codes (Section 113 (1) second sentence of the Telecommunications Act) only, if the legal conditions for their use are met.

6.3 New rules for information on telecommunications inventory data

Following a decision by the Federal Constitutional Court, legislators have until 30 June 2013 to amend the procedure for requesting information on telecommunications inventory data. To this end, the Telecommunications Act and a couple of other laws need to be amended.

As a result of the Federal Constitutional Court decision of 24 January 2012 (see no. 6.2), the procedure for requesting information on telecommunications inventory data must be revised in parts. To this end, the Telecommunications Act will have to be amended, as will the Code of Criminal Procedure (*Strafprozessordnung* (StPO)) and the respective laws governing the intelligence services, the Federal Criminal Police Office (*Bundeskriminalamt* (BKA)), the Federal Police (*Bundespolizei*) and the Customs Investigation Service (*Zollfahndungsdienst*) (see box for no. 6.3).

The transition period set by the court during which the current law may continue to be applied ends 30 June 2013, so the laws will have to be amended quickly. The Federal Ministry of the Interior started carrying out the court's requirements in summer 2012. The legislative process was not yet finished by the time this report went to press.

The current draft is mainly limited to implementing the court's requirements.

I have been involved in the legislative process from the start and was able to gain acceptance for some proposed amendments. Although the planned amendments will certainly help with data protection, I would have liked to see this opportunity used to question once again the general need to request information on inventory data and the very broad scope of the provisions on the procedure. I will therefore continue to critically monitor the progress of the legislative process and will work in particular to see that information on IP addresses to prosecute administrative offences is provided only in serious cases. I am also working to improve the authorities' obligation to inform data subjects.

Box for no. 6.3

With regard to the Telecommunications Act, the main emphasis is revising Section 113 to make it easier to understand. In the draft version, subsection 1 lists the data that telecommunications providers must disclose when asked. In addition to the data explicitly mentioned in the current law (i.e. inventory data pursuant to Sections 95 and 111 of the Act and data which protect access to devices or other storage systems), the draft for the first time explicitly refers to information on subscribers assigned an IP address at a particular time. According to this draft, the automated analysis of traffic data which is needed to provide this information is permitted. Subsection 2 of the draft version states that telecommunications providers may provide information only, if the authority requesting the information refers to a legal basis for the request which explicitly allows the relevant data to be collected. This provision thus implements the court's required "double-door" principle, which states that the telecommunications provider must be authorized to transfer the data and the authorities must be authorized to request the data (see no. 6.2). Subsections 3 and 4 of the draft version list the categories of those who are in principle authorized to request information and also state that telecommunications companies must not disclose the circumstances under which the information is provided. The only planned amendment not required by the court is found in subsection 5, which

requires companies with more than 100,000 customers to provide an electronic interface to process information requests. This is intended to make data transfer more secure and enable the clear identification of those requesting information. To make sure that the procedure does not amount to a disguised version of the automated information request procedure, as is the case with Section 112 of the Telecommunications Act, telecommunications providers are obligated to manually review every request received via the electronic interface.

The draft legislation adds a new Section 100j to the Code of Criminal Procedure allowing the relevant data (Section 113 Telecommunications Act) to be requested if necessary to investigate the facts of a case or determine the whereabouts of a suspect. Data needed to access devices or other systems may be requested only, if the legal conditions for using the data are met. The Code will also cover information on IP addresses assigned at a particular time (draft Section 100j (2) StPO), as in the relevant provision in the Telecommunications Act.

The provisions on requests for information will also have to be amended in the specialist legislation. The draft legislation therefore provides for amending the laws on the police at federal level (Act on the Bundeskriminalamt (*Bundeskriminalamtgesetz* (BKAG)), Act on the Federal Police (*Bundespolizeigesetz* (BPolG)) and on the intelligence services (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 (*Bundesverfassungsschutzgesetz* (BVerfSchG)), Act on the Military Counterintelligence Service (*Gesetz über den Militärischen Abschirmdienst* (MADG)) and Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst* (BNDG)) and the Act on the Customs Investigation Service (*Zollfahndungsdienstgesetz* (ZFdG)). Almost identically worded provisions are intended to enable requests for information on inventory data in the relevant areas of responsibility. Here too, information on data enabling access to devices or storage systems will be allowed only, if the legal conditions for using the data are met.

6.4 Telecommunications Act: What takes longer is not necessarily better!

The Telecommunications Act had to be revised in order to implement two European directives. In the process, data protection provisions were improved, but some amendments were made which are somewhat problematic.

The Act to Amend Telecommunications Law (*Gesetz zur Änderung telekommunikationsrechtlicher Regelungen*) entered into force on 10 May 2012 (Federal Law Gazette I 2012 p. 958 et seqq.). This amendment of the Telecommunications Act implements European law that had already entered into force on 19 December 2009 and should have been enacted in national law by 25 May 2011. Two major changes to the law, the introduction of special reporting obligations for telecommunications companies and more detail in the provision on location data, are discussed elsewhere in this report (see no. 3.5.3 and no. 6.5).

It is disappointing that the introduction of a uniform retention period for traffic data stored for the purpose of billing between service providers called for in the Federal Government's draft of the law was deleted at the last minute, and this without (official) explanation. At my initiative, retaining these data was to be allowed for no longer than three months after the other service provider had been billed. Unfortunately, the old provision remains unchanged, and the data may be stored for up to six months after billing, if the service providers provide evidence of need (see also no. 6.7).

Other amendments have led to less clarity rather than more. One such amendment concerns the scope of the data protection provisions in the Telecommunications Act in Sections 91 et seqq. These provisions protect subscribers' and users' personal data processed by service providers in connection with their commercial provision of telecommunications services. Providers of commercial telecommunications services are defined as anyone who provides partly or fully commercial telecommunications services or is involved in providing such services. In the amended version, the legal definitions of subscribers and users in Section 3 no. 14 and no. 20 of the Act were changed to refer only to the use of publicly accessible telecommunications services. The general consensus is that this was probably an error on the part of legislators resulting from the editorial revision in line with the European directives. The scope limited according to the legal nomenclature can be interpreted by analogy to mean that it is in principle open to closed user groups and not limited to providers of publicly accessible telecommunications services. This is important because, according to the Act, service providers include those who offer telecommunications services only to closed user groups. For example, hotels or cafés that offer their customers Internet access are service providers, as are employers who allow their employees to use the workplace telecommunications infrastructure for private purposes.

Section 92 of the Act was deleted; this provision allowed service providers to transfer personal data to bodies abroad in accordance with the Federal Data Protection Act (*Bundesdatenschutzgesetz* (BDSG)) only where necessary to provide telecommunications services, produce and send invoices or combat misuse. This provision thus contained a subject-specific purpose limitation to be observed in addition to the BDSG. In future, Sections 4b and 4c of the BDSG will govern such data transfers. It is not yet clear what the specific impact of this change will be. Data traffic within and among European Union member states is now to be treated exactly like domestic data traffic. Now the BDSG applies to data transfers to countries outside the European Union, known as third countries. I assume that this change will not lower data protection standards even for data transfers to third countries, especially since Section 4c (2) of the BDSG makes me responsible for authorizing transfers of personal data to third countries.

6.5 Mobile phone tracking

The latest amendment of the Telecommunications Act created regulations for mobile phone tracking services making it much more difficult to misuse these services – at least in theory.

I described the situation concerning tracking services at length in my 23rd report (no. 6.2). I was especially critical of the possibility of tracking without the knowledge of the mobile phone user. The amended Section 98 of the Telecommunications Act, which entered into force in May 2012, introduced stricter rules for tracking services: They must send an information text to the mobile phone whenever they identify its location; it is not necessary to send a text only, if the phone's location is not displayed anywhere but on the phone itself.

A few months after the new rules went into effect, I did some random checking on the Internet to see how they were being implemented. I found two companies that still appeared to be tracking mobile phones without sending texts. This is an offence subject to an administrative fine, so I asked the responsible agency, the Bundesnetzagentur, to look into the matter further.

The companies claimed that the mobile phone users were "tracking their own phones", so no text needed to be sent. This explanation did not convince me or the Bundesnetzagentur, because the location is not displayed on the phone but

somewhere else, so there was no reason not to send a text. The Bundesnetzagentur issued a fine, which was appealed. I will continue to follow the case with interest.

Another amendment to data protection law is significant for the identification and use of location data. Previously, the Telecommunications Act only covered location data collected or used in a telecommunications network. The amended Telecommunications Act now covers also those location data collected or used by a telecommunications service (see Section 3 no. 19 of the Act). This includes not only the cells to which a mobile phone is assigned, but possibly also the location data collected by satellite or WLAN tracking. The practical consequences of this change are not yet clear, but two sets of problems are already apparent: Firstly, it is often difficult to distinguish between a telecommunications service and a telemedia service, so that it is not clear whether the Telecommunications Act applies in a given case or whether it is the Federal Data Protection Act or the Telemedia Act. Secondly, tracking may be conducted by a service provided via the (mobile) Internet from abroad, so that German law may apply and be enforceable only to a limited extent.

Apart from these legal requirements, I am in favour of effectively limiting the burgeoning use of location data, especially in smartphone apps, and making it transparent for data subjects. Here, the providers of apps, companies offering download platforms and makers of smartphone operating systems have a responsibility to take action. I expect the EU's General Data Protection Regulation, which is currently under discussion (see no. 2.1.1), to provide significant improvement in this area, especially since it will require third-country providers to comply with European data protection law.

6.6 Emergency call tracking: Christmas always comes so unexpectedly ...

Emergency call tracking was supposed to go into effect on Christmas 2012, at least according to legislators. But technical problems are leading to delays.

The Telecommunications Act provided already in 2004 for identifying the location of emergency calls and sending this information to the rescue coordination centre. This is the only way to respond to emergency calls made from mobile phones, if the caller is unable to provide an exact location. For calls made from landlines, the location can be identified by network operators using inventory data. To implement this provision of the Telecommunications Act, the Emergency Call Ordinance (Notrufverordnung) and the Technical directive on emergency calls (Technische Richtlinie Notruf (TR

Notruf)) were needed; both took a long time. Thereupon in 2006, the Björn Steiger Foundation took the initiative and created an alternative system for locating emergency calls. This system has meanwhile been taken over by the Allianz OnlineService GmbH (AOS) (see 23rd Report, no. 6.2). Although this system enables emergency callers to be located, it does not comply with the law and does not rule out the possibility of misuse.

The Emergency Call Ordinance was enacted with some delay in 2009 and the Technical directive on emergency calls was finally published in the Bundesnetzagentur's official journal (No. 12) on 22 June 2011 (Administrative Order No. 42/2011), to be implemented by 23 December 2012 following an 18-month transitional period. Thus, emergency call tracking in compliance with the law was expected to go into operation by Christmas 2012.

Mobile network operators ran into technical problems during implementation procedures, so that parts of the Emergency Call Ordinance had to be amended (see also Bundesrat printed matter 595/12). Though everyone involved tried hard to implement the system quickly, it was impossible to do so by the deadline. Because the manufacturers of the emergency call answering points were informed of the changes to the technical directive very late, it will probably take several more months until the location data can be analysed in the rescue coordination centres. For this reason, I have agreed to let the AOS emergency call tracking system continue operating until the end of March 2013. I assume that the emergency call tracking system will be operating in compliance with the law by Easter at the latest.

The technical directive on emergency calls leave some questions open. For example, there is the demand that location information be transferred also in case of connections between network operators. Of course it makes sense to identify the location of callers who are using Internet telephony (VoIP), for example. But the possibility of "nomadic" use means that the caller's location is not necessarily the caller's home address. So the Internet service provider must be identified using the IP address and asked for location information. The technical directive does not explain how this is to be done at reasonable expense for any Internet service providers while ensuring sufficient protection against misuse. I am not yet aware of any solutions.

The technical directive also covers an optional procedure for additional transfer of location data for emergency calls made from mobile phones. This location

information, for example from a satellite, can be much more precise than location information from mobile networks. Transferring this additional information would certainly be useful since it could help save valuable time when responding to emergencies. However, callers should be informed of this and should at least be able to choose whether these data should be transferred or not.

Further, I find problematic the demand to equip emergency call lines with the "malicious caller identification" function. This function, which allows call recipients to trace calls they consider malicious, is likely to provide limited added value in identifying nuisance callers as most emergency call lines already have caller ID. The technical directive says nothing about how long traffic data may be stored, so I expect that the issues surrounding emergency calls will continue to occupy me in the future.

6.7 Guide to storing traffic data

From a guide to accessing data to a guide to storing traffic data: It is intended to ensure the uniform interpretation of the Telecommunications Act in compliance with data protection law.

The Munich public prosecutor general's office published a "Guide to Accessing Data Particularly in the Field of Telecommunications" which aroused considerable public interest in knowing how long traffic data are actually retained. Telecommunications providers faced criticism which was partly justified. This topic was therefore discussed at the "Jour Fixe Telekommunikation", a regular meeting of the Federal Commissioner for Data Protection and Freedom of Information with the data protection officers of network operators, in autumn 2011. As a result, I elaborated, together with the Bundesnetzagentur, a draft guide on storing traffic data. The network operators were asked to comment on an initial draft presented in spring 2012. The final version of the guide was published in autumn 2012. The guide is intended to ensure a uniform interpretation of the Telecommunications Act in compliance with data protection law – also in the sense of "best practises" - and represents a standard for checking the need to retain data.

I have published the guide on my website (in German only, under Informationsmaterial / Arbeitshilfen), and the Bundesnetzagentur published it in its official journal.

De facto seven-day rule

One common thread running through the guide is a de facto seven-day rule for storing traffic data not relevant for billing purposes. Over the years, this rule has proved to be a practical way to meet the requirements of both data protection and network operators.

On the basis of this rule reported malfunctions can be checked quickly and comparisons can be made over several days. A Federal Court of Justice decision (of 13 January 2011, III ZR 146/10) supported the seven-day rule in the case of storing dynamic IP addresses. If data are no longer needed to detect and remedy malfunctions before the seven days are up, they must be deleted by the company. Thus the seven days represent the maximum period of retention, and data may be deleted sooner depending on the specific circumstances.

There is a similar problem with regard to detecting misuse. In an exception from the purpose limitation principle, in this case data may be used for purposes other than those for which they were stored. In certain cases, it may be appropriate to store additional traffic data for a limited time. But the relevant provision in the Telecommunications Act has led to a great deal of discussion; in any case, Section 100 (3) of the Act yields no instructions that are not subject to debate. More details here would be desirable. The storage of raw data is the third area where the seven-day rule is applied. Section 97 (3) of the Act states that the data needed to calculate service charges must be identified “without delay”; this may at first sight be interpreted as “immediately”. However, it should be noted that in practice, the data are typically processed in several steps in complex data processing systems which have often been put together over many years and have to deal with many different billing rates. Improperly calculating billing charges would result in major financial losses to the companies. This is why the raw data are stored intermediately for a limited time. I believe that a maximum retention period of seven days is appropriate here as well, because with careful monitoring problems with data processing should be noticed within a few days. In my view, a longer retention period no longer constitutes “identification without delay”.

How long for billing?

The length of time data relevant for billing are stored was also examined. Section 97 (3) of the Telecommunications Act sets the maximum length of storage at six months

from the time the bill is sent. This much time is often not necessary, especially when service providers give customers, in their general contract terms, a maximum of eight weeks from receipt of the bill to object to any charges, in accordance with Section 45i (1) of the Act. As a result, I believe that three months (eight weeks plus processing and delivery time) is usually sufficient; justified exceptions may be made. Data can and must also be deleted in less than three months, if they are no longer needed for billing purposes. I also believe the six-month (or longer) retention period used by many providers for billing between network operators is inappropriate. In my view, there are usually no convincing reasons for this retention practice. A storage period of six months might be necessary only in certain justified cases, such as certain value-added services.

What does one need for billing?

Another issue is the content of data records. Particularly in mobile telephony, billing records contain a great deal of information, such as the cell used and the serial number of the mobile phone. Keeping a record of the cell makes it possible to track the caller's movements, but is not needed for billing except in the case of very few customers. Network operators cite the costs of having to change their highly complex above-mentioned systems, but here the law has priority: Data which are not or no longer needed for permitted purposes must be deleted.

6.12 Deutsche Post AG

6.12.1 The Deutsche Post DHL Data Privacy Policy (Konzerndatenschutzrichtlinie): A long haul

The Data Privacy Policy covers the legal transfer of data from the European Union to non-EU countries (third countries). Implementing the approval granted is taking longer than expected.

In my last report (see 23rd Report, no. 10.1), I referred to the completion of the approval process at European level. When I approved the "Deutsche Post DHL Data Privacy Policy (Konzerndatenschutzrichtline)" in February 2011 and gave the written approval to the board, I assumed the policy would be implemented within the company without delay. This approval gave Deutsche Post DHL (DP-DHL) the right to transfer personal data abroad according to the terms of its Data Privacy Policy

without having to request permission in each individual case. It was thus the first German company whose Binding Corporate Rules (BCR) were recognized following a comprehensive consultation procedure among the EU's data protection authorities.

My approval was (supposedly) a major step on the long road to finally implementing the BCR. But the company's internal procedures apparently took so long that I did not receive a copy of the Data Privacy Policy in a form that could be distributed throughout the entire company and define the applicable data protection standard there until the end of the reporting period. The final phase of implementation, namely sending the declaration of accession to the international members of the Deutsche Post DHL group, started in November 2012. Deutsche Post AG plans to have completely implemented its Data Privacy Policy in the course of 2013. I am certain this will happen, not least due to the assurances given by Deutsche Post AG, but I will no longer try to predict when.

7 Internal security and criminal law

7.1 Evaluating security legislation

Evaluating security legislation remains one of the core challenges of data protection. The Federal Government has not sufficiently evaluated the Act Supplementing the Counter-Terrorism Act; the evaluation of the Act on Setting up a Counter-Terrorism Database is not yet completed. I asked the German Research Institute for Public Administration to produce a guide for future evaluations. This guide is now available to all interested persons.

Security legislation governs powers which often infringe heavily on the fundamental rights of data subjects. Examples include undercover investigative measures such as telecommunications surveillance and broad powers of the intelligence services which leave individuals with few possibilities of legal redress. Such new powers are often granted hastily in response to current events or threats. For this reason, thorough reviews at regular intervals are needed to find out whether these powers have proved effective, necessary and proportional. I have therefore repeatedly called for comprehensive evaluations of the security legislation (see 23rd Report, no. 7.1.1 for a detailed discussion). In the process, it is also important to consider not only the effects of a single law, but also the interactions between the legislative instruments chosen ("overall account of surveillance"). Using a comprehensive assessment of all relevant facts, an evaluation must analyse all effects on data subjects, including

indirect ones. Analysing the status quo can also be helpful ahead of planned major reforms. It is first necessary to find out whether existing legislation has been properly enforced in the past, priorities have been set appropriately and resources used in a targeted way. Only then is it possible to decide whether and what legislative steps are necessary (see no. 7.7.6).

Those granted the additional powers should not have a role in interpreting the results of the evaluation; instead, the German Bundestag should decide, on the basis of independent evaluations conducted using scientific criteria, whether options adopted once continue to be justified. I am therefore critical of the Federal Government or a federal ministry conducting such evaluations.

For example, in 2011 the Federal Ministry of the Interior presented its own evaluation of the Act Supplementing the Counter-Terrorism Act (*Terrorismusbekämpfungsergänzungsgesetz* (TBEG)) for which it had hired external methodological expertise. The report was insufficient in terms of substance, too. It did not focus on the Act's impact on the fundamental rights of affected individuals. But precisely this focus was needed to be able to judge the proportionality of the powers. The evaluation should have answered the question whether the Act achieved the intended aims and whether legislators had chosen the mildest appropriate instrument in each case. But the report does not even make sufficiently clear what it is actually based on. In particular, it is not apparent whether at least individual cases were thoroughly evaluated as examples. In general, the authors addressed the fundamental rights of affected individuals only superficially. At the time this report went to press, no final evaluation of the Act on Setting up a Counter-Terrorism Database (*Antiterrordateigesetz* (ATDG)) had been presented; the deadline was 31 December 2011. Nor is there a report on the evaluations provided for in the Coalition Agreement (see 23rd Report, no. 7.1.1). The government commission for this purpose was not convened until early January 2013 and will hardly be able to carry out this task with the necessary thoroughness during the time left in this legislative term.

As a result of the negative experience with the evaluation of the Act Supplementing the Counter-Terrorism Act, legislators created after all a new clause on evaluation (Act Amending 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 (*Gesetz zur Änderung des Verfassungsschutzgesetzes*)). The new clause requires explicitly evaluating how

often the intelligence services use the powers granted them by this Act to infringe on the fundamental rights of persons affected, and what the impact of such infringement is. This evaluation is to be checked against how effectively the intelligence services have used these powers to detect or fight terrorist activities. I hope the new clause improves the future evaluation at least of this Act in future.

To help with future evaluations, I commissioned the German Research Institute for Public Administration to produce a guide on conducting ex-post evaluations of legislation with special attention to data protection. This guide was completed in late 2012. It is intended for all those who wish to request legislative evaluations or are familiar with them, in particular members of parliament, researchers and civil servants. The guide thoroughly treats the standards, instruments and methods which apply to evaluation and presents the framework conditions under constitutional law. It also provides a practical overview of the necessary steps to be taken by the agencies to be evaluated. Even before an evaluation is requested, the guide helps decision-makers define the proper conditions for evaluation.

Link to the guide (in German): http://www.datenschutz.bund.de

7.2 Counter-terrorism database

The Federal Constitutional Court had critical follow-up questions regarding the Act on Setting up a Counter-Terrorism Database. My checks indicate that significant data protection deficits remain, also in fundamental respects.

On 6 November 2012 the Federal Constitutional Court (*Bundesverfassungsgericht*) heard a constitutional complaint concerning the Act on Setting up a Counter-Terrorism Database. At the court's request, I presented my criticism of the Act (see 21st Report, no. 5.1.1) at the hearing and reported on my experience with checks. In particular, I suggested calling on legislators to define various provisions of the Act more narrowly and precisely and make them more proportional in order to protect innocent (contact) persons. The court addressed critical questions to representatives of the Federal Government and the relevant agencies also concerning the provisions I had criticized. No court decision had been made by the time this report went to press. I expect the decision will have consequences for the database on right-wing extremism (RED; see no. 7.3), which has almost identical content as the counter-terrorism database.

My checks indicate there were (see 23rd Report, no. 7.1.2) and are significant problems with compliance with data protection law. For reasons of confidentiality, among others, I can describe these here only in abstract terms and as examples:

– The Military Counter-Intelligence Service (*Militärischer Abschirmdienst* (MAD)) has stored “dolose” contact persons (i.e. persons aware of planned terrorist acts or those that have been committed; see 22nd Report, no. 4.2.2.2) in the counter-terrorism database without having its own information to justify this storage and valuation (see Section 2 of the Act) (on the problems with storing information on contact persons, see 22nd Report, no. 4.2.2.2 and 21st Report, no. 5.1.1). MAD explained that a different agency had stored the data subjects in the counter-terrorism database characterizing these persons as (dolose) contact persons. MAD’s action violates Section 2 first sentence of the Act, which states that data stored in the counter-terrorism database must be collected by the agency that stored it, as described in the explanatory memorandum to the Act. According to the explanatory memorandum, only (additional) intelligence that the storing agency already is disposing of may be stored. In MAD’s view, this requirement cannot be derived from the explanatory memorandum. The discussion of this point is ongoing.

– In a free-text field of its counter-terrorism database source file, the Federal Intelligence Service (*Bundesnachrichtendienst* (BND)) had stored information in violation of the law. During my inspection, the BND agreed to delete the information in question and fill out these fields in compliance with the law, so I refrained from making a formal complaint.

My check of the counter-terrorism database also revealed that the BND had stored a file on a German national employed by a major German company as a dolose contact person in both the counter-terrorism database and the relevant BND source file.

During my inspection, the BND conceded that there were no files on this case. In response to follow-up questions, during the inspection the BND said that the company had asked the BND whether the person in question was known by the BND. After checking the BND informed the company that the person in question was not known by the BND. The BND could not explain how this request for information resulted in the person being added to the database as a dolose contact, especially as it had no further information on the person.

During my inspection, I asked the BND to block the person's data until I had completed check procedures; instead, the data were deleted, supposedly by mistake, after my control. The Federal Criminal Police Office (*Bundeskriminalamt* (BKA)), which is responsible for the database log files, refused to grant me access to these files.

After the inspection, the BND wrote to me describing the matter differently than it had during my inspection: The BND wrote that an information had not been requested by the company and that none of the person's data had been transferred to the company. Instead, according to the BND, the request had come from a foreign government office and had been answered. The BND was unable to provide any supporting documents.

This change in the situation has serious legal consequences for the data subject: If it supplies information to the company, the BND would be required to inform the person in question, but it is not required to do so when supplying information to a foreign public body.

During my inspection, I had screenshots made of the what I could see on the viewing screens concerning the person's data stored in the database. These screenshots corroborate the original, oral account of the BND that the information request came from the company and which was answered by the BND. I therefore told the BND to inform the person in question. After intensive discussions, the BND agreed to do so, but the Federal Chancellery, which is responsible for expert supervision of the BND, said it was not required to inform the data subject and ordered the BND not to do so. I objected. I had not received a response from the Federal Chancellery by the time this report went to press.

I provided these and other results of my inspections to the Federal Constitutional Court as requested. Several of the state commissioners for data protection also reported the results of their inspections to the court.

7.3 Database on right-wing extremism

Like its model, the counter-terrorism database (see no. 7.2), the database to fight right-wing extremism is a joint database of the police and intelligence services. Although the database on right-wing extremism includes some improvements over

the counter-terrorism database, I still see an urgent need for legislative action. My initial checks have already found violations.

The legal basis for the new database is the Act to Improve the Fight Against Right-Wing Extremism (*Gesetz zur Verbesserung der Bekämpfung des Rechtsextremismus* (REDG)), which has much the same content as the Act on Setting Up a Counter-Terrorism Database (see 21st Report, no. 5.1.1). A new feature is that the data in the database on right-wing extremism may be analysed for use in projects (see Section 7 REDG). The Act entered into force on 31 August 2012.

According to information from the Federal Ministry of the Interior, the database on right-wing extremism is intended as the "second pillar [along with the Joint Centre for Countering Right-Wing Extremism (*Gemeinsames Abwehrzentrum gegen Rechtsextremismus* (GAR)); (see no. 7.7.6] to improve information-sharing between the police and intelligence services". To this end, the Act obligates 36 federal and state security agencies (Federal Criminal Police Office (BKA), Federal Police, Federal Office for the Protection of the Constitution, Military Counter-Intelligence Service, the state offices for the protection of the Constitution and the state criminal police offices) to store their data on violent right-wing extremism in the database on right-wing extremism. The BKA is in charge of running the database, which officially went into operation on 19 September 2012.

The Federal Ministry of the Interior calls the RED database "a right conclusion to draw from the NSU murders, because communication between the authorities needed certain improvements here and there". Given that the investigations of the NSU's activities and of possible deficits on the authorities' side as well as of the main reasons for them (see no. 7.7.6) is still under way, I find this statement premature. The right conclusions can be drawn only after a complete and thorough investigation of all the circumstances and causes. If members of the security authorities don't (or won't) recognize that a crime has a right-wing extremist background, they will not store this information in their agency's relevant database, and so it will not be entered into the central database on right-wing extremism. It is important to realize that the RED database will not remedy shortcomings in enforcement.

I also pointed this out in my comments as expert witness at the public hearing of the German Bundestag's Committee on Internal Affairs on 19 March 2012 regarding the Act to Improve the Fight Against Right-Wing Extremism (REDG) (see Printed Paper of the Bundestag Committee on Internal Affairs 17(4)460E). At the hearing, I also

criticized the reference to the “successful” operation of the counter-terrorism database since 2007 as a reason for establishing the database on right-wing extremism. I found no valid basis for this assessment, before the evaluation of the Act on Setting up a Counter-Terrorism Database, which is required by law, has been carried out (see no. 7.1).

I was also concerned that the Act to Improve the Fight Against Right-Wing Extremism was adopted before the Federal Constitutional Court had ruled on a constitutional complaint concerning the Act on Setting up a Counter-Terrorism Database (see no. 7.2). If the latter was found to be unconstitutional even in part, this would have major consequences for the identical provisions of the former.

As I explained in my comments to the Federal Constitutional Court, certain provisions of the Act to Improve the Fight Against Right-Wing Extremism must be defined more narrowly and precisely and be more proportional in order to protect innocent (contact) persons.

I also reported on my experience with checking the database on right-wing extremism. In checks conducted at the Federal Criminal Police Office (Bundeskriminalamt (BKA)) and the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz* (BfV)) a few days before the oral proceedings, I found that everyone the BfV had stored in the RED database as dolose contact persons should have been entered as non-dolose contact persons (on the question as to when a contact person is to be considered “dolose”, see 23rd Report, no. 7.1.2). This has major consequences for the data subjects. While only so-called basic data may be stored in order to identify non-dolose contact persons (e.g. surname, first name, address, date of birth, etc.; see Section 3 (1) No.1 (a) of the Act on Setting up a Counter-Terrorism Database), additional data, so-called extended basic data, may be stored on dolose contact persons (see Section 3 (1) No. 1 (b) of the RED Act; see box for no. 7.3). During my inspection visit, the BfV agreed to make corrections immediately.

I also found during my checking that, based on a catalogue of criteria agreed with other agencies, the BfV systematically transfers to the database on right-wing extremism data which are not supposed to be stored there. Because this catalogue is classified, I cannot report on it here in further detail and thus cannot mention the specific data (categories). However, I can say that the data concerned are highly

sensitive and that I did not expect them to be systematically transferred to and stored in the right-wing extremism database.

These findings - and others - demand additional inspections, also in order to determine the dimensions of the problems. I was unable to conduct these checks before this report went to press. A final assessment will be possible only after having conducted such checks.

Box for no. 7.3

Extended basic data (Section 3 (1) (1) (b) of the Act to Improve the Fight Against Right-Wing Extremism

These include very extensive data, such as telecommunications connections and devices used by the data subject or third persons, e-mail addresses, bank account information, lockers, vehicles registered to or used by the data subject, information about educational degrees, occupational training and occupation, information about current or former activity in a vital institution, language skills, summary special remarks, additional information and assessments and much more (see Section 3 (1) (1) (b) (aa) through (uu)).

7.4 Federal Criminal Police Office

7.4.1. Telecommunications interception at the source

I have found problems with so-called telecommunications interception at the source.

I have checked the telecommunications surveillance conducted by the Federal Criminal Police Office (*Bundeskriminalamt* (BKA)), Customs Criminal Office (*Zollkriminalamt* (ZKA)) and Federal Police for compliance with data protection law (concerning the ZKA, see 23rd Report, no. 7.4). I found shortcomings in the technical safeguards and the mechanisms for deleting information gathered from the core area of private life. By the time I checked, 40 operations involving telecommunications interception at the source had been conducted (see box for no. 7.4.1).

The streams of intercepted data were insufficiently secured using an inadequate encryption mechanism. Nor were there adequate measures to ensure that the persons and systems involved in the technical processes were securely authenticated. Together with other information, the existing log files made it possible to track activity and data retrieval but did not meet the requirements given in Section 20l (2) second sentence in conjunction with Section 20k (3) of the Act on the Federal Police Office (*Bundeskriminalamtgesetz* (BKAG)). I submitted a formal complaint to the Federal Ministry of the Interior and the Federal Ministry of Finance concerning this matter. Penetrating a computer can create security breaches which allow third parties to break into the system. This is why data streams must be securely encrypted, and why only authorized persons and systems should have access to the data (authentication). I found evidence that both of these mechanisms were inadequately implemented in the surveillance software and that the key was easy for third parties to find.

But I was not able to conduct a precise technical analysis. The source code of the software used was not documented. The BKA made an effort to persuade the software maker to provide me with the source code. However, the software maker wanted my staff to sign a confidentiality agreement and demanded a significant amount of money for the use of its staff; I refused to agree to these conditions. My authority to inspect can be restricted only by law. A confidentiality agreement would also interfere with my statutory reporting obligations, for example my obligation to report to the German Bundestag. I had not entered into a contract with the software maker, nor is it subject to my data protection supervision. If the agency under review cannot provide the source code for the purpose of checking compliance with data protection law, then I am unable to conduct such checks.

In checking, I looked carefully at the technical system and the information gathered. The documents and files I saw showed no indication that the authorities had used the software to collected any data beyond current communications or had conducted further surveillance of the users. In particular, I found no screenshots, user files or the like.

I was able to check the measures' compliance with the law only to a limited extent. Where the authorities conducted measures on behalf of public prosecutor's offices of the states, I was authorized to check only as far as the federal authorities had discretionary powers. I was able to view the necessary court orders indicating that the measures were authorized. I do not assess the content of court orders out of

respect for judicial independence. In terms of legal policy, however, I see no legal basis for these measures in criminal investigations. The relevant provision of the Code of Criminal Procedure (*Strafprozessordnun*g (StPO)) does not provide for using software to secretly penetrate computers. The same is true of the law applying to the customs authorities.

The law only refers to conventional forms of telecommunications surveillance in which telecommunications providers intercept conversations by order of the security authorities. The Federal Constitutional Court explicitly noted the additional risks associated with telecommunications interception at the source in its decision on so-called remote searches of computer hard drives and called for special statutory provisions on such intrusive measures. But federal legislators have so far created the necessary legislation on remote searches of computer hard drives and telecommunications interception at the source only for the BKA with regard to the area of international terrorism, not in the StPO, which is the relevant code for criminal law enforcement. This has led to the unusual situation in which the BKA has farther-reaching powers for threat prevention than for law enforcement.

I also find the technical mechanisms for deletion insufficient where content from the core area of private life is concerned. Such content concerns the most intimate areas of highly personal communication, such as conversations with close confidants about one's emotions. I found such content in the files of the BKA. I was not allowed to judge their deletion, as this was the responsibility of the public prosecutor's office of the state concerned. I did inform the responsible state commissioner for data protection. But the BKA was responsible for the deletion mechanism itself. Using this mechanism, it was possible only to delete the entire conversation, not the part related to the private sphere.

The Federal Ministry of Finance accepted my report as constructive. The Federal Ministry of the Interior also commented on my report, but does not agree with my concerns about compliance with the law. However, it does see room for improving the software.

The federal and state governments are currently working on a standardized specification of services intended to define key elements; it will apply when security authorities buy or develop new software for surveillance purposes. On the drafts submitted so far I have made my comments to the Federal Ministry of the Interior; in particular, I have insisted that the data protection authorities must have unconditional

access to the source code in order to check compliance with data protection law. In addition, the software's functions should be clearly defined, especially with regard to what constitutes current telecommunications and what does not.

Box for no. 7.4.1.

In telecommunications interception at the source, the investigating authorities secretly install software on the targeted person's computer. If this person communicates with others using this computer, the relevant data are intercepted by the investigating authorities. Communications include, for example, encrypted conversations where the targeted person is using the IP-phone software "Skype". This measure is restricted to the current communication, i.e. the software used by the police authority may not transfer any other content stored on the computer, such as texts, images or other files to the police authority. In this way, telecommunications interception at the source differs from remote searches of computer hard drives.

7.4.2. Preventive counter-terrorism measures

The BKA has already used its new powers to prevent international terrorist threats, though only in a few instances.

Effective 1 January 2009 the BKA was given new powers and responsibilities to prevent international terrorist threats (Section 4a and Sections 20a through 20t of the BKA Act. I asked the BKA whether it had already used these new powers and if so, how extensively.

The BKA replied that the new powers had so far been used only in a few cases: in major operations in which the BKA carried out a number of measures, some of which it regards as low-threshold. This applies in particular to the powers provided for in the general clause on data collection, questioning, verification of identity and searches of persons and property (Sections 20a through 20f BKA Act). No statistics on this are available. The BKA gave me concrete figures for measures taken under Sections 20g through 20n of the BKA Act. The BKA used special means of data collection (such as long-term surveillance, eavesdropping on private speech outside homes) in a double digit range. The number of telecommunications surveillance measures and retrievals

of traffic data was slightly more. The BKA also conducted three surveillance operations of a home and six remote searches of computer hard drives.

The new powers also include telecommunications interception at the source. I have already conducted an initial data protection inspection of such measures (see no. 7.4.1). I will continue to monitor the development of the other measures (see also no. 7.4.6).

7.4.6. Cell enquiries

Data from cell enquiries are also stored at the BKA.

I asked the Federal Criminal Police Office (Bundeskriminalamt (BKA)) how many times it had requested traffic data occurring in a specific radio cell (see box for no. 7.4.6; Resolution of the Data Protection Commissioners of the Federation and of the Länder of 27 July 2011) and how much data resulting from such requests it had stored. The BKA provided a very thorough response, so I initially postponed the data protection inspection I had originally planned. The BKA also asked me for data protection advice on storing data from cell enquiries in various databases which it created in the course of current investigations in a large-scale proceeding. I am still advising on this issue. The BKA stores data from cell enquiries in various internal databases that are used in working on individual investigations. Some of these databases have large quantities of traffic data, most of which were collected by the state police before the BKA assumed responsibility for the investigations. These data are not deleted until after the related investigation has been closed; as a rule, this is not until after a final sentence has been handed down or the case has been permanently dismissed. The BKA notes that the public prosecutor's office is responsible for making this decision for each case.

As part of his investigation into cell enquiries, the Data Protection Commissioner for the State of Saxony asked me to ask network operators for some information about the data transferred. The result was as expected: Data are collected only in the course of telecommunications proceedings, and only traffic data without inventory data are transferred. So I was very surprised when my colleague in Saxony informed me that in 2009 a mobile network operator had also transferred a significant amount of inventory data in response to cell enquiries. This was confirmed by the company in response to my follow-up question. The company said that it had changed procedures and stopped sending inventory data in response to queries of traffic data

only when implementing the Federal Constitutional Court ruling on preventive data retention in 2010. Incredibly, the company was unable to say how long inventory data had been provided without asking. The company thought the practice had been in place at least since 2005. I have therefore issued a formal complaint to the Bundesnetzagentur regarding the company.

Box for no. 7.4.6.

Resolution of the Data Protection Commissioners of the Federation and of the *Länder* of 27 July 2011

Cell enquiries must be contained!

With the help of cell enquiries, law enforcement authorities in Dresden collected hundreds of thousands of mobile phone traffic data during public rallies and counter-demonstrations on 19 February 2011, including the telephone numbers of callers and those they called, the time of day and information about cells where mobile phone activity took place. In this way, the authorities collected information on the movements and communications behaviour of tens of thousands of demonstrators, including members of state and federal parliaments, lawyers and on-duty journalists as well as residents of the densely populated centre of Dresden.

This incident demonstrates the weakness of the current law.

The legal basis for non-individualized cell enquiries is Section 100g (2) second sentence of the Code of Criminal Procedure, which states that, “in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice” to allow the authorities to obtain traffic data from the telecommunications services providers. This provision is linked to a general subsidiarity clause. This provision, which was added to the Code of Criminal Procedure in 2001, is inadequate: It is not sufficiently defined, nor does it reflect the current technical situation. Today’s devices generate a large quantity of traffic data without any action on the owner’s part; these data can then be collected in a cell enquiry.

Cell enquiries constitute a covert intrusion on the secrecy of telecommunications (Article 10 of the Basic Law). They affect all owners of mobile telephones registered in a particular cell, not only certain individual suspects, as in the case of telecommunications surveillance pursuant to Section 100a of the Code of Criminal Procedure. Such enquiries reveal the type and circumstances of communications by as many as tens of thousands of persons who have given no cause for government intervention. Further, they create the ability to prosecute these persons unlawfully on grounds other than those for which the enquiry was made, such as violations of the law on assemblies. In relation to individuals, cell enquiries are a tool for generating suspicion. The Code of Criminal Procedure does not specify how the authorities are to handle the data collected, in particular how long, on which persons and in what other connections the police may use these data.

The Federal Constitutional Court has always stressed that traffic data can reveal a great deal about an individual's communications behaviour. Traffic data can reflect the social network of the person in question; they can reveal links to political parties, trade unions or civic action groups.

The Conference of Data Protection Commissioners of the Federation and of the *Länder* therefore calls on federal legislators to limit the scope of cell enquiries concerning more than single individuals, to ensure that the principle of proportionality is followed more closely in practice, to strengthen the principle of necessity (for example, by requiring the immediate reduction of data collected to those necessary for prosecution or court proceedings) and to specify the provisions on deletion in Section 101 (8) of the Code of Criminal Procedure in greater detail.

7.4.7 Public searches on the Internet

The Conference of Data Protection Commissioners of the Federation and of the Länder addressed the issue of police appeals for public help on the Internet, particularly in social networks. The Federal Criminal Police Office also has a page for such appeals on "Facebook".

Numerous federal and state agencies operate their own websites, some have a Facebook "fanpage" (see no. 5.8.2). Discussions focused in particular on police authorities using the social network to publish alerts. Public searches are a particularly severe intrusion on the privacy rights of the persons concerned. On the Internet, information is delivered to an unlimited audience anywhere in the world.

Currently, information once published on the Internet cannot be completely “fetched back”. Therefore, a public search on the Internet should always be a measure of last resort to be considered only for particularly serious offences. It would be especially problematic if police were searching not only for suspects but also for witnesses on the Internet. Information published online should be limited to what is strictly necessary. I am also very concerned about information provided by citizens being made public on the website of the investigating agency (e.g. in forums, chats, social networks, and the like). Publishing suspicions in this way is always inappropriate, especially if the person concerned later turns out to be innocent.

The Federal Criminal Police Office (*Bundeskriminalamt* (BKA)) has its own fanpage with “Facebook”. It has shown great restraint, however, as this page has so far been used only in investigating members of the “National Socialist Underground (*Nationalsozialistischer Untergrund* (NSU))”, which involves very serious crimes. Police appeals for help from the public which are published on Facebook need to meet not only the special requirements of criminal procedure, however; it is above all necessary to ask how the data of those visiting the page are handled (user data). The BKA has taken measures to limit negative impacts in terms of data protection law: It has deactivated the bulletin board and sharing functions in its public appeals and the sending of messages. The Facebook page itself does not actually contain the appeal information but rather links to the BKA website. This minimizes visitor data but does not keep cookies from being placed or IP addresses being sent to Facebook via the “Like” button. “Facebook Insights” also conducts use analysis without asking.

The Conference of Data Protection Commissioners of the Federation and of the *Länder* wrote to the Conferences of the Ministers of the Interior and of the Ministers of Justice to point out the following key points:

– The police must first determine whether they can set up their own websites before taking advantage of social networks.
– If they find that using their own websites is not sufficient, they must choose a network operator which complies with German data protection law.
– The police or public prosecutor in question must be able to meet their obligations under data protection law (master of proceedings). This applies to the initial publication of the appeal and to its further treatment, such as deletion. It must be completely clear which data the network provider processes.

7.5 Customs

7.5.1 Employee screening for AEO certification in customs administrations

Employee screening ordered by customs administrations, often without reasonable suspicion of wrongdoing, for so-called Authorized Economic Operator (AEO) (= "Zugelassener Wirtschaftsbeteiligter") certification continues to be problematic. Even a recent decision by the Federal Finance Court (Bundesfinanzhof (BFH)) does not resolve these concerns.

AEO certification is intended to simplify the process of clearing customs. It applies to companies based in the European Union involved in cross-border goods traffic. Any economic operator based in the EU which meets the criteria for compliance with customs regulations (appropriate book-keeping, financial solvency and appropriate security standards) can be issued an AEO-F certificate ("Customs simplifications / Security").

As part of the AEO certification process, the customs administrations require the companies applying for a certificate to conduct extensive employee screening, in some cases repeatedly and at short intervals, which I have already criticized on numerous occasions (see for example 23rd Report, no. 13.7). For this screening, employees of the company applying for a certificate must undergo a background check in which they are checked against so-called anti-terror lists. Checks are conducted using the sanctions lists (lists of names of persons suspected of belonging to a terrorist organisation) referred to in the EC counter-terrorism regulations (Regulation [EC] No. 2580/2001 and No. 881/2002). But the UN terrorist lists on which the lists of these EC Regulations are based are questionable in terms of the rule of law, because they are not compiled in a transparent way and because the listing is subject to judicial review only to a limited extent (see European Court of Justice decisions of 15 November 2012, C-539/10; C-550/10 P; C-417/11 P). Because the lists are subject to errors and because the consequences of being found on the list can be heavy for the data subject, procedural safeguards in the form of data protection rights for data subjects are indispensible.

In spring 2011, I inspected the practices of a main customs office (*Hauptzollamt* (HZA)) in issuing the above-mentioned AEO-F certificate and raised objections. The office granted AEO-F certificates only if the companies applying for them demonstrated that they regularly and systematically checked their employees against

the EC lists of suspected terrorists. In doing so, the HZA violated no. 253 of the service instruction “Zugelassener Wirtschaftsbeteiligter- AED” of 22 June 2010, which limits background checks of employees to those in security-relevant areas, and thus also violated the principle of proportionality. According to its supervisory authority, the Federal Ministry of Finance, the office in question has admitted the error and remedied it.

In its resolution of 22-23 November 2011, the coordinating body of the supreme supervisory authorities for data protection in the private sector, known as the Düsseldorf Group, calls for effective limits on employee screening and demands that data not be subject to blanket screenings in the absence of reasonable suspicion of wrongdoing (see box for no. 7.5.1).

In the meantime, the decision of the Federal Finance Court (decision of 19 June 2012, VII R 43/11) represents the first clarification of certain disputed points related to employee screening by the highest court with jurisdiction. However, this decision is not convincing from the perspective of data protection law, because the court found that Section 32 (1) first sentence of the Federal Data Protection Act (*Bundesdatenschutzgesetz* (BDSG)) allowed the personal data of persons employed by companies which have applied for an AEO certificate to be checked against lists of suspected terrorists. Although the court did limit screening to employees in security-relevant areas, this does not address my criticism of the blanket, mass screening of employees ordered by customs administrations without specific suspicion, because fundamental doubts about the procedure are at stake. For example, I find it questionable whether these company-internal checks add anything to counter-terrorism efforts, given that employees are paid via bank transfer and banks are already required under Section 25c of the Banking Act (*Kreditwesengesetz* (KWG)) to check their clients against the lists of suspected terrorists. In the end there is no viable legal basis for checking data on such a mass scale. Neither the EC anti-terror regulations nor the relevant UN resolutions contain such obligations. Nor does the general clause in Section 32 of the Federal Data Protection Act seem to apply here.

Box for no. 7.5.1

Resolution of the Supreme Supervisory Authorities for Data Protection in the Private Sector

(Düsseldorf Group, 22-23 November 2011)

Effectively limiting employee screening for AEO certification

The Düsseldorf Group has repeatedly addressed the problem of employee screening, most recently in its resolution of 23-24 April 2009. There is reason to address this issue once again.

In recent years, the customs administration in particular has started requiring companies to extensively screen their employees – and in some cases third parties – in order to qualify for a certificate as an Authorized Economic Operator (AEO) (= "Zugelassener Wirtschaftsbeteiligter"). In some cases, blanket screenings are conducted at intervals of only a few weeks, in the absence of reasonable suspicion of wrongdoing and without differentiation. These screenings are already conducted by specialized service providers who take advantage of companies' uncertainty; this is also the reason why these screenings are conducted with growing frequency. In the practical experience of the supervisory authorities, there is a lack of clear rules on how to deal with the results of data screening (hit management). Although the Federal Ministry of Finance on 14 June 2010 issued rules limiting this practice, however, the responsible customs authorities do not implement them uniformly.

In its resolution mentioned above, the Düsseldorf Group finds that such screenings are permissible only on the basis of specific legislation. Such a legal basis is lacking.

Neither the EU anti-terror regulations nor other sanctions lists satisfy the requirements for such a specific legal basis. These regulations contain only the general obligation not to extend any legal advantages to the persons and institutions listed in the annexes. They do not, however, require anyone to screen employees, clients or suppliers.

The Federal Government agrees that the anti-terror regulations do not require any systematic checks of employee files against sanctions lists without reasonable suspicion of wrongdoing. According to the Federal Government, such checks are permissible only in line with due diligence obligations and differentiated according to fields of business and risk levels. The Federal Government believes it is up to the companies to decide how to ensure compliance with the anti-terror regulations (Bundestag document 17/4136 of 3 December 2010).

With this in mind, the Düsseldorf Group recommends and insists on the following:

– Companies should not conduct blanket data screening without reasonable suspicion of wrongdoing. Because wages and salaries are paid only via bank transfer and credit institutions are required by Section 25c of the Banking Act to check their customers against the lists of suspected terrorist, there is no need for companies to conduct such checks of employee data.
– The customs authorities are called on to comply with the rule of law in the AEO certification process. Uniform practices under the rule of law offer companies legal certainty.
– We ask the Federal Government to submit current AEO certification practices to a comprehensive evaluation in the near future.

7.6 Federal Police

7.6.2 Illegal transfer of personal data to Europol

For years, the Federal Police illegally provided the Europol Information System with personal data of persons smuggled across borders.

In the course of fulfilling its tasks the European Police Office “Europol” is operating various information processing systems (see no. 2.2.2), one of which is the Europol Information System (EIS). Information may be stored in this system only of persons suspected or convicted of crimes or of persons regarding whom there are factual indications to believe they will commit a crime over which Europol has jurisdiction (Article 12 (1) in conjunction with Article 4 of the Council Decision 2009/371/JHA establishing the European Police Office).

As my inspection of the Federal Police showed, data transferred to Europol were based exclusively on cases of “human smuggling”. In every case (I checked), the Federal Police had entered into the EIS not only the persons suspected of smuggling humans, but also the persons smuggled. This is not in accordance with Council Decision 2009/371/JHA. The reason for the error was the highly inflexible technical process used at the time, in which it was possible to send to Europol either all the personal data related to a certain case or none. The Federal Police should have noticed this problem years ago, as - starting in 2007 - I repeatedly informed them of improper entries in EIS. But nothing was done.

During my inspection, I also found that the special provision in the Council Decision on deleting data was not used in practice. This provision states that if “proceedings against the person concerned are definitively dropped or if that person is definitively acquitted, the data relating to the case in respect of which either decision has been taken shall be deleted” (Article 12 (5) of Council Decision 2009/371/JHA). However, the data were not deleted, even though the Federal Police said that they are usually informed by the public prosecutor’s office of the results of the proceedings. Here, too, a remedy was needed to ensure that special provisions on deletion in accordance with Section 12 (5) of the Council Decision were applied in all regional offices of the Federal Police.

The Federal Police responded immediately to my inspection. They immediately stopped entering information into the EIS and deleted all records already submitted to the EIS. In the meantime, the system was modified so that it is now possible to submit only the permitted data to the EIS. Old and new records of personal data are now checked to see whether they may be transferred to the EIS. The Federal Police also made sure that the data of a person concerned are deleted from the EIS when proceedings are definitively dropped or the person is definitively acquitted.

I welcome the Federal Police’s immediate and full response to my findings. As a result, I refrained from making a complaint under Section 25 (2) of the Federal Data Protection Act. Nevertheless, the technical shortcomings of the system should have been detected much earlier, which would have prevented the rights of data subjects from being infringed upon and reduced the aggravation and effort for the Federal Police.

7.10 Money Laundering Act

Numerous amendments have been made to the law on money laundering which are problematic from the perspective of data protection law.

The 2011 re-enactment of the Money Laundering Act

The Act to Optimize the Prevention of Money Laundering of 22 December 2011 (*Gesetz zur Optimierung der Geldwäscheprävention* (GWPräOptG)), Federal Law Gazette I p. 2959) made extensive changes to the Money Laundering Act (*Geldwäschegesetz* (GwG)) mainly intended to remedy shortcomings of the Financial

Action Task Force on Money Laundering (FATF) located at the OECD. In addition, the number of suspicious transaction reports filed under the Money Laundering Act reached a new high in 2011: 12,868.

The amended law made stricter and expanded the due diligence and reporting obligations as well as internal safeguards; it also expanded the group of persons and institutions covered by the law and reduced the threshold for suspicious transactions. In tightening the due diligence obligations (the obligation to verify the identity of contracting partners, among others), the law significantly expanded the data collection and storage obligations of those covered by it (see box for no. 7.10). And the heavy fines for violations of due diligence obligations are likely to increase the pressure to collect more data than required and supply it to the Federal Criminal Police Office (Bundeskriminalamt (BKA)) and other law enforcement authorities.

For example, due diligence obligations (and the related reporting obligations) must now be met even for money transfers valued at EUR 1,000 or more, when outside a business relationship. Also the amended Money Laundering Act no longer requires specific grounds to suspect acts of money laundering or terrorist financing; the existence of facts indicating such acts is sufficient. Further, persons and institutions covered by the Act are supposed to inform the Federal Criminal Police Office and the relevant law enforcement authority early on of any unusual or conspicuous business relationships with relevance for money laundering. Reports are now required even in “low-risk” cases; only the extent of identity verification and monitoring can now be reduced.

Increased due diligence obligations as to politically exposed persons

The amended Act also increases due diligence obligations with regard to so-called politically exposed persons (PEP) and significantly expands the scope. I objected to this for reasons of data protection already during the legislative process. In my view, these increased obligations are justified only in cases in which increased risk can in fact be assumed. In the legislative process, my calls for a solution which pays more attention to fundamental rights, at least with regard to PEPs holding office within Germany, were at least partly heard.

I am also extremely critical of the widely used “PEP lists” compiled and sold by commercial services. These lists usually combine various information, such as name, aliase, date of birth, nationality, place of residence, career, current position, family

and business relationships, photos, etc. European data protection authorities are not able to check lists compiled by foreign services so that there is no control whether the collection of the data is taking place in compliance with the rule of law. Although the instructions for interpretation and use from the Customs Criminal Office (*Zollkriminalamt* (ZKA)) state that such commercial PEP lists do not have to be used, foreign lists are regularly used in practice.

Changes in electronic money transactions

The group of persons and institutions covered by the law was also expanded for electronic money transactions, and the ability to make anonymous electronic payments was severely restricted. During the legislative process, I was nonetheless able to tone down the extensive obligation to verify the identity of customers buying electronic money (especially pre-paid cards), as was originally planned. Now the identification and due diligence obligations apply only when the amount of electronic money stored on a device is more than EUR 100 per calendar month. When determining the maximum amount of EUR 100, there are still some uncertainties that could result in more personal data being collected than is required by law. It would certainly help if the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin)) would clarify how to manage this in practice.

Preventing money laundering even in legal gambling

Under the Act Supplementing the Money Laundering Act (*Gesetz zur Ergänzung des Geldwäschegesetzes* (GwGErgG)), providers of legal Internet gambling and the credit and payment institutions hired by them must ensure comprehensive monitoring, too. In this way, the above-mentioned re-enactment of the Money Laundering Act extends the increased due diligence and reporting obligations to the gambling sector.

Box for no. 7.10

Section 6 Money Laundering Act - Enhanced due diligence

(1) In possible situations of higher risk of money laundering or terrorist financing, the institutions and persons covered by this Act shall apply enhanced due diligence

measures appropriate to the higher risk. Section 3 (4) second sentence and (6) shall apply mutatis mutandis.

(2) It is to be considered that a higher risk is emanating in particular in the following cases and thus the following enhanced due diligence measures shall be carried out:

1. Institutions and persons covered by this Act shall take appropriate risk-based measures to determine whether the contracting party and, if existing, the beneficial owner, is a natural person who is or has been entrusted with prominent public functions, or immediate family member or person known to be closely associated to such a person as defined in Article 2 of Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of “politically exposed persons“ and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214 of 4 August 2006, p. 29). As a rule, public offices below the national level are not considered prominent public functions unless their political significance is comparable with those at the national level. Institutions or persons covered by this Act obligated to clarify whether the contracting party or beneficial owner is a close associate of a person who has been entrusted with prominent public functions must do so only if this relationship is known to the public or if the institutions or persons covered by this Act have reason to believe that such a relationship exists; they are, however, not obligated to conduct investigations. If the contracting party or beneficial owner is a politically exposed person as defined here, the following shall apply:

a) establishing a business relationship through an intermediary acting on behalf of institutions or persons covered by this Act shall be subject to approval by a supervisor of the intermediary;

b) appropriate measures shall be taken to determine the origin of assets to be used in the business relationship or transaction; and

c) the business relationship shall be subject to intensified continuous oversight.

If the contracting party or the beneficial owner assumes a prominent public function only during the course of the business relationship, or if the institution or person covered by this Act becomes aware that the contracting party or the beneficial owner

exercises a prominent public function only after the business relationship has been established, continuing this business relationship shall be no longer subject to approval by a supervisor of the intermediary but by the institution or person covered by this Act. For clarification matters the contracting party shall provide the necessary information for the institution and person covered by this Act and shall inform them of any changes without delay as long as they maintain a business relationship. If the contracting party or the beneficial owner is a politically exposed person exercising a prominent public function in Germany or as a Member of the European Parliament elected in Germany, or if the contracting partner or the beneficial owner has not exercised a prominent public function for at least one year, the general due diligence obligations pursuant to Section 3 shall apply subject to a risk assessment of the individual case.

8.14 Anti-Doping

Data protection in the fight against doping in sport continues to be an important and controversial issue at national and international level.

The Article 29 Working Party reactivated its WADA subgroup, of which my staff are members, in response to current international developments, such as the World Anti-Doping Agency's (WADA) announcement in early 2011 that it had made significant changes to its Anti-Doping Administration and Management System (ADAMS) (see 22nd Report, box for no. 5.9) and the process of revising the WADA Code which started in 2012.

In February 2012, the Article 29 Working Party sent a letter prepared by its WADA subgroup to the responsible EU commissioner describing the problems with data protection in WADA's anti-doping system. Before that, the European Commission had expressed its support for anti-doping measures which comply with EU law and uphold fundamental rights, including the right to data protection. The Article 29 Working Party believes that athletes' consent to drug testing cannot serve as the legal basis for processing their personal data. The Working Party also notes that data can be transferred from the EU to the ADAMS database and from there to other third countries only if the country of destination guarantees an adequate level of data protection or if the conditions for derogations under Article 26 of the Data Protection Directive are met. The Working Party remains very critical of the fact that penalties issued for doping violations are published on the Internet, and finds this neither necessary nor proportional. Lastly, the Working Party calls on WADA to examine the

proportionality of collecting information on athletes' locations in order to conduct drug testing without prior notice ("whereabouts information") and at least to reduce the length of time these data are stored.

Both the WADA Code and the accompanying standards, in particular the International Standard for the Protection of Privacy and Personal Information (ISPPI), have been under revision since early 2012. The revisions shall be completed by the end of 2013. In the context of the revising process, the Article 29 Working Party will check whether the criticisms from its earlier opinions (Working Paper 156 of 1 August 2008 and Working Paper 162 of 6 April 2009) were addressed in the draft revisions and will notify WADA in writing of any remaining data protection concerns as necessary.

9 Financial matters

9.1 CDs containing tax data

The debate on the use of unlawfully acquired CDs containing tax data is still continuing. It seems doubtful whether making it a crime to handle stolen data will help.

Without a doubt, buying information on tax data held abroad is lucrative for the tax authorities and helps the government increase its revenues significantly at a time of financial crisis. Also in view of the constitutional principle of equitable taxation, the aim and enforcement of taxation in line with Article 3 (1) of the Basic Law, which states that all should be equal before the law, seems at first glance to be a reason for buying CDs containing tax data, since it can help, to a certain extent, to discourage people from hiding assets abroad and to make it possible to pursue tax evasion more effectively.

But it is necessary to remain within the limits of the rule of law, because the government is ultimately enlisting the help of criminals who have collected the data by actually having stolen them. I have repeatedly stressed the need for a special legal framework to reconcile the conflicting interests appropriately (see most recently 23rd Report, no. 9.1). It makes no difference that the Federal Constitutional Court and the responsible tax courts did not object in principle to using such CDs in a criminal investigation (Federal Constitutional Court, decision of 9 November 2010, 2

BvR 2101/09) or in tax proceedings (Cologne Tax Court, decision of 15 December 2010, 14 V 2484/10; Hamburg Tax Court, decision of 12 October 2011, 3 V 117/11), because the purchase of CDs with stolen tax data still falls within a legal grey area and is subject to significant consequences under criminal law, as demonstrated by the Swiss authorities who recently issued arrest warrants for German tax inspectors.

The issue is not yet resolved at last instance. The German courts of lower instances have so far operated on the assumption that the tax officials in question have violated neither German criminal law nor international law (see Düsseldorf Regional Court, decision of 11 October 2010, 4 Qs 50/10; Bochum Regional Court, decision of 7 August 2009, 2 Qs/09). In particular, they ruled that German tax authorities may buy the data on the basis of their general powers of investigation. From the perspective of data protection, however, such a broad interpretation of these powers is problematic and creates the possibility of arbitrary action by the authorities. Referring to general powers of investigation to justify buying the tax data is not convincing, given the serious infringement of the confidentiality of personal data, and it thus would trivialize the data theft. The rule of law and the general principles of data protection demand that any legal basis, when shaping the basis of interference, should define the intended use precisely and for a specific area and should ensure that the data are appropriate and necessary for this purpose (Federal Constitutional Court, judgment of 15 December 1983, 1 BvR 209/83, among others).

However, I am not convinced by the current addition to the Criminal Code proposed by the justice minister of the state of Hesse which would make it a crime to handle stolen data (draft Section 259a of the Criminal Code (*Strafgesetzbuch* (StGB)). From the perspective of data protection, I certainly welcome efforts to improve protection for personal and other data which have been obtained unlawfully (such as passwords or other access codes) by adding a central provision to the Criminal Code. Making it an offence according to general criminal law to buy and acquire unlawfully collected data could therefore be a sensible addition to existing law (Sections 43 and 44 of the Federal Data Protection Act (*Bundesdatenschutzgesetz* (BDSG)). However, I find it difficult to explain why an exception should be made for governments to do so with impunity – a lex tax CD?

9.2 Tax identification number

I fear that efforts to further expand the use of the tax identification (tax ID) numbers risk turning it into a general identification code for individuals, which would violate the Constitution.

In previous activity reports I have repeatedly had to address the problems with tax identification (tax ID) numbers from the perspective of data protection law (see most recently 23rd Report, no. 9.2). This is necessary again in the present report. Tax ID numbers serve as unique identifiers of taxpayers when assessing taxes. Given the constant growth in the electronic transfer of tax data to the tax administration, tax ID numbers are intended to enable these data to be matched to a specific individual (for example in notices concerning pension benefits or control reports). The aim is to ensure fair taxation and to prevent possible misuse.

In this context, the Federal Finance Court (*Bundesfinanzhof* (BFH)) found tax ID numbers in compliance with the Constitution, as the public interest in fair taxation justified the infringement on the right to informational self-determination (BFH, judgment of 18 January 2012, II R 49/10), although the strict principle of purpose limitation and necessity must be observed. Legislators are therefore not free to expand the use of tax ID numbers as they please, because the requirements of data protection law which are also anchored area-specifically in Section 139b (2) through (5) of the German Fiscal Code (*Abgabenordnung (AO)*) draw strict boundaries.

But others, such as employers, pension insurance funds, providers of social services, health insurance funds, financial institutions and child benefit funds already use tax ID numbers in other, albeit narrowly defined, contexts. I will continue to oppose the extended use of tax ID numbers. Anyhow, the Federal Ministry of Justice and I were recently able to remove unnecessary reference to the use of tax ID numbers from a Federal Ministry of Finance draft for an ordinance on issuing and amending tax ordinances.

Issuing new tax ID numbers in the case of adoptions and witness protection programmes

Under current law, one tax ID number is supposed to be issued only once for each natural person in order to ensure that the assignment of numbers is sufficiently permanent and clear. Although this principle certainly makes sense, it brings with it

significant risks in certain cases, if no exceptions can be made. In the case of adoptions, transsexuals or persons in witness protection programmes, the tax ID number would make it possible to trace the person's former identity. But this would violate the special protection guaranteed to these sensitive data, for example in the Federal Data Protection Act (Bundesdatenschutzgesetz (BDSG)), the Act to Harmonize Protection for Witnesses (*Zeugenschutz-Harmonisierungsgesetz* (ZSHG)), the Gender Recognition Act (*Transsexuellengesetz* (TSG)) and also by the confidentiality of adoption.

The right of individuals to informational self-determination based on Article 2 (1) in conjunction with Article 1 (1) of the Basic Law (*Grundgesetz*) also includes the right to manage one's own identity. In cases when personal data need special protection, other constitutional values (adoption - Article 6 Basic Law; witness protection - Article 2 (2) Basic Law) can increase the entitlement to protection, so that appropriate legislative measures are to be taken. In the cases mentioned above, keeping the same tax ID number for one's entire life could lead to critical gaps in protection, especially since there is no guarantee that tax ID numbers will not be widely used and distributed. However, in cases where changing identity features is justified, it should not be possible to reconstruct a previous identity in this way, as is clear from the legal valuations. I therefore find it advisable to enact legislation allowing a new tax ID number to be issued in the cases mentioned above (adoption, transsexuals, witness protection).

Tax identification: Carved in stone?

At the moment, deleting a tax ID number assigned in error is unnecessarily difficult. A petitioner who has held only French citizenship since 1997 asked me to make sure that the Federal Central Tax Office (*Bundeszentralamt für Steuern* (BZSt)) deleted his tax ID number. At the request of his health insurance provider, the BZSt issued the petitioner a tax ID number even though he was no longer subject to taxation in Germany and thus no tax ID number should have been issued.

I therefore asked the BZSt to delete the number and inform the petitioner. The BZSt agreed to do so, but said that it was currently impossible to delete tax ID numbers, as the necessary procedure was still being developed. Section 20 (2) no. 1 of the Federal Data Protection Act clearly states that personal data are to be deleted if their storage is not permitted. The controller of the data is required to have the necessary procedures in place to meet this obligation. These technical and organizational

measures are necessary to ensure that data protection complies with the law. The BZSt has not sent final word on deleting the tax ID number. I will continue to monitor the situation critically.

10 Business and transport

10.1 Smart electricity meters need smart data protection

Data protection solutions are in sight for the use of "smart" digital electricity meters. While the Energy Industry Act has established a framework, an ordinance is still needed to specify the details.

The Federal Government's decision to promote the use of renewable energy sources, known as the *Energiewende*, is a major economic and environmental challenge. The use of smart meters also turns it into a data protection issue. Consumption data can be used to draw conclusions about consumers' habits and lifestyles. This is why I advocate solutions which - without sacrificing functionality - respect users' rights to informational self-determination.

The Energy Industry Act

I have already discussed the data protection challenges raised by the use of smart meters for all parties involved (see 23rd Report, no. 5.1). The amendment of the Energy Industry Act (*Energiewirtschaftsgesetz* (EnWG)) in June 2011 was a first major step. The data protection provisions in the Act call for a strict purpose limitation on the use of sensitive consumption data as well as for binding standards for data security. In Section 21g of the Act, I was able to have a conclusive list of purposes included for which collecting, processing and using personal data are allowed. Section 21g of the Act defines which bodies are authorized to use the data and makes clear that data protection principles such as data reduction and data economy also apply to personal data used in connection with smart metering systems.

However, the Act only provides the outline for data protection; the details are to be specified in an ordinance. I hope that this ordinance will also pay appropriate attention to data protection concerns.

Guidelines for smart metering in compliance with data protection law

In June 2012, the Conference of the Data Protection Commissioners of the Federation and of the *Länder* adopted a resolution and additional guidelines on smart metering in compliance with data protection law (see box for no. 10.1). These are intended to help legislators in drafting the ordinance. The guidelines provide recommendations on designing technical systems for smart metering in compliance with data protection law. Based on so-called use cases, the guidelines describe how to implement in practice the central data protection requirements of purpose limitation, data economy and necessity.

Data protection requirements in connection with the introduction of smart grids and meters are being discussed not only in Germany. In March 2012, the European Commission issued a “Recommendation on Preparations for the Roll-out of Smart Metering Systems” (COM(2012) 1342 final). The recommendation calls for ensuring that smart metering systems provide full privacy protection when processing personal data. The Commission also renewed the mandate of its “Smart Grids” Task Force established in late 2009. The work programme for 2012 of the Task Force’s second expert group calls, inter alia, for developing a Data Protection Impact Assessment (DPIA) for smart grids.

Represented by the members from France and of the United Kingdom and by the European Data Protection Supervisor, the Article 29 Working Party participates as an observer in the meetings of this expert group and will comment on the final version of the DPIA when it is finished. The technology subgroup under my supervision will draft the recommendation (see no. 2.4.1.2).

Box for no. 10.1

Resolution of the Conference of the Data Protection Commissioners of the Federation and the *Länder* of 27 June 2012

Guidelines for smart metering in compliance with data protection law

Smart energy grids and meters are a vital component when it comes to ensuring sustainable energy supply in the interest of resource-saving, environmentally friendly and efficient generation, distribution and use of energy. The Conference of the Data Protection Commissioners of the Federation and of the *Länder* has adopted

guidelines setting forth recommendations for designing technical systems for smart metering in compliance with data protection law. The centrepiece of the guidelines is the description and evaluation of use cases from the perspective of data protection law. These use cases represent the individual components of data processing for smart metering and take into consideration the respective protection needed.

The data protection commissioners of the Federation and of the *Länder* believe it is essential to adhere in particular to the following principles:

– Processing of smart meter data must be restricted to the purposes listed in the Energy Industry Act.

– The reading intervals must be long enough that no information concerning end consumer behaviour can be derived from the consumption data.

– Whenever possible, smart meter data should merely be anonymized, pseudonymized or aggregated before transmission.

– It must also be possible to access high-resolution data locally at the end consumer without the consumer having to rely on external processing of such data.

– The number of data recipients should be as small as possible.

– Reasonable deadlines for deleting the data must be set in order to avoid data retention.

– The communication and processing steps of smart metering operations must be visible and demonstrable to the end consumer at all times. End users must be able to recognize and, if necessary, prevent access to the smart meter.

– Additionally, the consumers concerned must have an enforceable right to have data deleted or corrected and to object to data.

– End consumers must be able to choose a tariff which discloses as little information as possible regarding their lifestyles without jeopardizing their energy supply.

– Smart meters must not be accessible from outside the home. Clear-cut profiles must be defined for authorized access to data. Indications can be found in the

requirements in the Protection Profile and in the Technical Guideline of the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* (BSI)).

– The technical systems must be conceived and designed to ensure data protection (Privacy by Design). The technical equipment must provide end consumers with all the information, options and control possibilities needed to enable them to control their energy consumption and manage their privacy at a level not falling short of the state of the art. It is especially necessary to create legally binding specifications for hardware design of devices, processes and infrastructures as well as for their use.

10.5 Cooperation between the German and the American authorities responsible for overseeing auditors

The German commission responsible for overseeing auditors (Abschlussprüferaufsichtskommission (APAK)) and the US Public Company Accounting Oversight Board (PCAOB) have signed a memorandum of understanding on cooperation.

Since 2005, APAK has independently exercised public expert supervision of the Chamber of Auditors and thus over all auditors and certified public accountants. In 2011, the PCAOB approached a number of European countries with the aim of concluding bilateral agreements allowing European authorities responsible for overseeing auditors to transfer data to the PCAOB.

At European level, Directive 2006/43/EC on statutory audits of annual accounts contains provisions on cooperating with the competent authorities of third countries. According to Article 47 of the Directive, the competent authorities of the Member States may allow the transfer of working papers to the competent authorities of third countries in cases of inspections and investigations of auditors, if the European Commission had declared them adequate.

In its Decision of 1 September 2010 (2010/485/EC), effective until 31 July 2013, the Commission decided on the adequacy of the competent authorities in the US, thereby satisfying the first condition for information-sharing between APAK and PCAOB (so-called “adequacy decision”).

Under Article 2 (4) of the Decision, Member States must in addition ensure “that the bilateral working arrangements which allow the transfer of audit working papers or other documents held by statutory auditors or audit firms between their competent authorities and the competent authorities of ... the United States contain appropriate safeguards with regard to the protection of personal data”.

The Article 29 Working Party (see no. 2.4.1) wrote to the Commission to recommend what authorities responsible for overseeing auditors should do until a final, common European solution has been reached: They should use a “Memorandum of Understanding – (MoU)” from the European Group of Auditors’ Oversight Bodies (EGAOB) as an interim solution.

The PCAOB did not accept this solution and concluded bilateral agreements with individual European countries (the United Kingdom, the Netherlands) already in 2011. It also approached Germany’s APAK in this regard. APAK kept me informed of how the matter was progressing and on 12 April 2012 signed an agreement with the PCAOB. Based on the Dutch agreement, this agreement includes a few additional modifications in terms of data protection. The bilateral agreements with the PCAOB signed so far (including that with APAK) all expire on 31 July 2013, as that is when the adequacy decision ceases to be valid.

I have attended proceedings in the Article 29 Working Party subgroup on financial matters. The Commission has agreed to check whether a common European solution is possible for the period after 1 August 2013 and will inform the Article 29 Working Party.

15 From my office

15.4 Visits from foreign delegations

Various data protection experts, in particular from Asia and Eastern Europe, have visited my office to discuss current data protection issues and share experience.

I received several foreign delegations at my office during the reporting period. Data protection experts from Japan and I have regularly shared experience for a number of years now. For example, experts from the Nomura Research Institute and professors from various Japanese universities came to find out more about the concept of data protection in Germany and our national experience with European

law. A delegation from the Justice Ministry of the Republic of China (Taiwan) discussed practical issues, such as declarations of consent to data processing on the Internet and how data protection is supervised in Germany.

Staff from my office have participated in events organized by the European Commission under the Technical Assistance and Information Exchange instrument (TAIEX) to support data protection authorities in the EU candidate countries and in the framework of the European Neighbourhood Policy (ENPI). At the request of the European Commission, I have also welcomed to my office in Bonn and my liaison office in Berlin delegations of the data protection authorities in Croatia, the Republic of Moldova and the Former Yugoslav Republic of Macedonia; I informed them about data protection in Germany, and we discussed current data protection issues relevant for both sides. A group from the Bulgarian data protection authority visited for a week of experience-sharing under the auspices of the EU's Leonardo da Vinci Programme.

Helping build up new data protection authorities abroad with experience gained in Germany, engaging in dialogue with our partners abroad and thereby gaining new insights remain important concerns of mine.

16 Important items from past activity reports

15. 23rd Report, no. 8.2.1 **Amending the Act on the Central Register of Foreigners**

In my last activity report, I reported on the start of the legislative process to implement the European Court of Justice decision in the case of Heinz Huber v. Germany (judgment of 16 December 2008, C-524/06). The court found that storing data on Union citizens in a central register like the Central Register of Foreigners (*Ausländerzentralregister* (AZR)) and transferring them to other authorities was lawful only subject to strict conditions. The draft amendment of the Act on the Central Register of Foreigners (*Gesetz über das Ausländerzentralregister* (AZRG)) presented by the Federal Ministry of the Interior did not fully comply with the court's requirements.

I was actively involved in the interministerial coordination process, which made significant improvements to the draft. The draft reduced the amount of data on Union citizens to be stored in the register (for example, photographs are no longer to be

stored) and specified that data could only be transferred for purposes related to foreigners or asylum law and only to authorities responsible for such tasks. The draft also made it illegal to provide information on groups of Union citizens. The amended Act was passed by the German Bundestag and the Bundesrat (Bundestag document 17/11051, 17/11364) and is to enter into force nine months after its promulgation. I will work to see that the changes are technically implemented in the central register soon.

Fortunately, the amended Act also includes a clause on research by the Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge* (BAMF)), thus satisfying a data protection request of long standing (see 21st Report, no. 7.1.3). The new clause provides in all clarity a subject-specific legal basis for the BAMF to use data from the central register for its attending research.