Activity Report for 2013 and 2014 of the Federal Commissioner for Data Protection and Freedom of Information 25th Activity Report -

1 Reform of European data protection law

1.1 General Data Protection Regulation nearing completion?

The Council of the European Union and the European Parliament have been negotiating the European Commission's proposal for a General Data Protection Regulation since January 2012. I have closely monitored this reform project over the past two years. The project has made significant progress during the reporting period, and the Regulation is expected to be adopted in 2015.

When presenting its proposals in 2012, the European Commission set the ambitious goal of adopting the General Data Protection Regulation before the European parliamentary elections in May 2014. Although this goal was not achieved, the project made such good progress in 2014 that the Regulation is likely to be adopted in 2015.

In my 24th Activity Report (No. 2.1.1), I commented at length on the Commission's proposal, its structure and evaluation from the perspective of data protection law.

Although it seemed doubtful at times whether European data protection reform would ever be realized, the European Parliament has made decisive progress with the reform project: Its Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) adopted a common position in October 2013 which was confirmed by the plenum of the Parliament in March 2014, thereby completing the first reading in the Parliament. To do so, the LIBE Committee reviewed nearly 4,000 requests for changes and compiled a compromise proposal. This proposal is remarkable also in terms of its content. Data protection authorities in Germany and Europe as well as civil society representatives have had a favourable opinion about most of the recommendations. In my view, they significantly improve the Commission's draft, which itself was headed in the right direction in many areas.

By contrast, the negotiations in the Council of the European Union have been much more difficult, which is understandable given the differing interests of 28 member states. However, the way large member states, including Germany, managed the negotiations did not lead at first to rapid discussion. But since the Parliament has come to an agreement, the Council has clearly been trying to achieve consensus with constructive and goal-oriented negotiations. Over the course of 2014, the Federal Government also increasingly lent its support.

The Justice and Home Affairs Council agrees in principle on various chapters and horizontal issues of the Regulation: These include the fundamental aspects of the marketplace principle (Art. 3 (2) of the Regulation; see No. 1.2.7 of this report); the transfer of personal data to third countries (Chapter V; see No. 1.2.6); the obligations of the controller (Chapter IV of the Regulation); and the applicability of the Regulation to data processing in the public sector (parts of articles 1, 6 and 21; see No. 1.2.1), including specific opening clauses for member states' national law (Chapter IX of the Regulation). Progress was also achieved on other chapters.

Despite this major development, considerable effort will still be required under the Latvian Council Presidency to reach agreement on the entire Regulation in June 2015.

Like my counterparts in Germany's federal states and in the other EU member states, I have offered constructive criticism in the data protection policy debate in order to draw attention to the fundamental rights of people in Europe.

For example, the 85th conference of the data protection commissioners of the Federal Government and of the States (Länder) expressed its position on various fundamental issues of the data protection reform in its resolution *Europa muss den Datenschutz stärken* (Europe must strengthen data protection; see Annex 3) and relevant explanations (see Annex 4). In another resolution on the structure of future data protection supervision in Europe, the 87th conference of the data protection commissioners of the Federal Government and of the States called for strong citizen-orientated data protection supervision, for efficient cooperation among data protection authorities and for legally binding powers for the future European Data Protection Board (see No. 1.2.5 below).

The Article 29 Data Protection Working Party has also addressed the General Data Protection Regulation on a regular basis. In addition to commenting on the decisions of the Justice and Home Affairs Council and on the so-called risk-based approach (see No. 1.2.3), it also focused once again on the future structure of data protection supervision and cooperation among data protection authorities (see No. 1.2.5).

In November 2014, the European Data Protection Supervisor in Brussels and I organized an event on the reform of European data protection law which was an excellent opportunity for an intensive discussion with high-ranking decision-makers on the progress of the negotiations and the remaining open questions.

In view of the global dimension of the processing of personal data and the resulting enormous challenges for data protection, I believe the reform of European data protection law urgently needs to succeed in the interest of citizens, but also in the interest of businesses and public administration. Only a strong European data protection law can respond to the challenges posed by the Internet, Big Data technologies, cloud computing and ultimately the sensory and electronic capture of all areas of life and thus have a global impact.

"You can forget about dessert. I can see from your bank account that you don't even have enough to pay for an espresso." The EU's General Data Protection Regulation: On holiday with data protection

Source: Greser & Lenz, rdv-online

1.2 Key individual aspects of the General Data Protection Regulation

The overall positive development is made up of many elements, the most important of which will be considered in greater detail below.

1.2.1 The General Data Protection Regulation should also apply to public administration!

The question whether the General Data Protection Regulation should also apply to the public sector, other than the area of law enforcement, now seems to have been answered in the affirmative.

As explained in my 24th Activity Report (No. 2.1.1), the European Commission followed the regulatory structure of the 1995 European Data Protection Directive, in principle including the public sector in the scope of the General Data Protection Regulation. The European Parliament did not question this approach in its decision of March 2014.

However, the negotiations in the Council showed that some member states, in particular Germany, are critical of this approach. This is understandable, given the fact that Germany has data protection law, especially for the public sector, that has developed over decades, with differentiated and sector-specific provisions, most of which the Federation and the federal states want to keep.

I have always supported the aim of preserving sector-specific data protection law in Germany as far as possible, where more precise formulations yielding the same or a higher level of data protection as the Regulation were concerned. However, I opposed removing the public sector from the scope of the Regulation. Instead, I advocated including the public sector in the Regulation and creating the necessary

leeway within the Regulation in order not to endanger the overall reform project (see 24th Activity Report, No. 2.1.1).

It was long unclear whether European law would even allow sector-specific data protection law to be preserved alongside a European regulation. Unlike the 1995 Directive currently in force, a regulation is directly applicable European law which no longer needs to be implemented in national law and does not allow such implementation. In its draft, the Commission left room for member state law to govern certain aspects of the processing of personal data in the public sector. In its proposal of March 2014, the European Parliament took up this approach and further specified the leeway for national laws. In the Council, too, a large majority of member states accepted including the public sector in principle in the scope of the Regulation.

To address the concerns of the Federal Government and the federal states, the Italian Council Presidency also pursued the basic approach of the Commission and the Parliament further and proposed a general opening clause for Article 1 of the Regulation. This clause is intended to enable the member states to retain specific rules or adopt new ones for data processing in the public interest or by authorities in carrying out public tasks. Concerns about whether such an opening clause complied with European law were successfully resolved. Unfortunately, the Council did not address the Federal Government's request (which I supported) to authorize member states to adopt rules creating a higher level of data protection than that provided by the Regulation.

Additional special opening clauses are to be created in Chapter IX; in view of the general opening clause, however, these additional clauses will cover only the balance between data processing and freedom of expression (see No. 1.2.2), the relation to freedom of information laws and on the re-use of information, data processing in the employment sector, data processing for scientific, statistical, historical and archival purposes, and data processing by churches and religious associations.

For Germany, a special focus was the processing of personal data by archives in the public interest. The point was not only to create a reliable framework for the future work of the federal and state (Land) archives, but also to address the special needs of the federal commissioner responsible for the files of the German Democratic Republic's Ministry of State Security (Stasi). In particular, it was necessary to make sure that data protection obligations – such as the right to be forgotten – did not conflict with the important public interest in the permanent preservation and availability of significant documents of (contemporary) history. The opening clause proposed by the Council will achieve this.

I agreed with the Federal Government that a high level of data protection is needed for the processing of personal data in the employment sector and that the protection of employees should, if possible, exceed the requirements of the Regulation. Here it became clear that the general opening clause for the public sector would not suffice, because data processing in the employment sector is largely conducted by businesses and other private entities. The Council therefore proposed a separate opening clause for this purpose, allowing the member states to further specify data processing in this context. Unfortunately, the Federal Government failed to gain support for its further-reaching proposal to enable member states to mandate a higher level of data protection.

The overall approach sketched out here was approved in principle by the Justice and Home Affairs Council in December 2014.

I believe the agreement in the Council represents a good compromise, on the basis of which most sector-specific data protection law in Germany and other member states can be preserved. As for the remaining critical points, I hope for improvements in the upcoming trilogue between the Commission, the Parliament and the Council.

1.2.2 Data protection in conflict with the freedom of expression?

Can a high court decision strengthening data protection at the same time weaken the freedom of expression and information? Some say yes and are therefore calling for a mechanism to settle disputes in order to find an appropriate balance between fundamental rights.

The judgment on the Google search engine (see No. 2.3.2) brought applause from data protection officials. I was pleased as well that, with its decision, the European Court of Justice (ECJ) once again recognized data protection as an important fundamental right which deserves protection, especially in today's increasingly digital and connected world. But the court's decision, which will extensively strengthen the protection of personal data, also drew criticism that it was too one-sided and would threaten the freedom of expression and information. When search engine results no longer display links to certain content, they argued, this could seriously limit the fundamental freedom of expression and information.

I do not share these doubts: The ECJ does not require articles and publications not to be found by using search engines; it is only supposed to become more difficult to find them by using a certain combination of search terms which must be specifically related to a certain person. For example, a search engine can continue to display links to a newspaper article if the search parameters do not include the specific person who requested that the link be deleted. Although this may make it more difficult to find certain content, it does not completely suppress it. Further, there is no legal claim that articles can be found in a search engine (see No. 2.3.2 for details).

And every decision to remove links requires a comprehensive assessment of all the rights of the concerned parties, which I believe is crucial. Such decisions must of course take into account the right of the person requesting that links be removed to control his or her personal information as well as the freedom of expression and information of third parties.

However, the Federal Ministry of the Interior apparently fears that the parties to the proceedings will not adhere to these principles, so it has called for including a dispute settlement mechanism in the General Data Protection Regulation: An independent, non-governmental office would verify in a legally binding way whether, in response to a request to remove links, the interests of the authors of the content concerned have received sufficient consideration and the fundamental rights of all parties have been properly balanced. The data protection supervisory authorities will certainly not be bound accordingly, so they may be consulted independently of such a dispute settlement mechanism and, as provided for by the ECJ, can assist persons requesting links to be removed in asserting their rights.

Although I principally do not have any objections to independent dispute settlement mechanisms, I do not see the need for such an arrangement. The Council of the European Union has already responded to the ECJ decision by amending the draft General Data Protection Regulation: Article 80, which already called for reconciling the fundamental rights in question, was expanded to include freedom of information as well as freedom of expression as rights to be reconciled with the right to the protection of personal data. The member states may provide for exceptions in their national law to certain chapters of the Regulation.

1.2.3 The risk-based approach

Since the consultations on the General Data Protection Regulation began, there has been intensive debate over whether to replace or at least supplement the current regulatory model for data protection with a risk-based model.

In the General Data Protection Regulation, the European Commission has used the same regulatory model as the European Data Protection Directive of 1995 and German data protection law: The processing of personal data is generally prohibited and is allowed only if the data subject has provided consent or if processing is allowed on a legal basis. This model has proved effective, because either data subjects

themselves may decide what happens to their data, or legislators must decide whether data processing is necessary and reasonable in the overriding public interest.

This model guarantees the autonomy of the individual and makes the processing of personal data somewhat more predictable and transparent. This is especially applying in the era of the Internet and Big Data technologies: The more confusing data processing becomes, the more important it is to have a transparent and understandable regulatory framework.

In the course of discussions of the reform of European data protection law, certain representatives of the business sector, of politics and of science have time and again questioned this model, saying that the general prohibition on data processing limits innovation and hinders Europe in the competition with other economic areas outside Europe. They say that the model creates major obstacles for small and medium-sized businesses in particular, while global Internet companies hardly follow these rules anyway. As one possible solution, a risk-based approach has been proposed which would generally allow the processing of personal data, at least in the private sector, and would prohibit or place regulatory restrictions only on data processing associated with special risks.

I oppose this kind of risk-based approach and have repeatedly made my opposition clear to my counterparts in Germany's federal states and in the Article 29 Working Party. Already in its decision on the population census of 1983, the Federal Constitutional Court made it clear that there were no longer any meaningless data in an era of automated data processing. Depending on the context or combination with other information, every piece of information about an individual may be both trivial and extremely revealing. This is hard to predict, which means it is difficult to make a standardized assessment of the risk. Legislators can only regulate the risks they know about. But this would not be compatible with the individual's fundamental right to protection.

A risk-based approach understood in this way would fundamentally undermine the protection of data subjects: Under current law, every new infringement of the right to determine the use of one's information in legislation and its application must be justified, both in terms of policy and in practice with every act of processing. This places the burden of justification on those who want to process the data. If this principle is reversed, then data subjects must explain why certain data processing is risky. This would seriously weaken their position.

In my view, the current model of data protection law, which the General Data Protection Regulation also follows, does not hinder innovative business models. The ability to innovate cannot mean that every technical solution and business model is permitted, with the law having to conform to that. Instead, technical solutions and new business models must find innovative ways to adapt to the existing regulatory framework, which certainly continues to develop. With its strict data protection law emphasizing fundamental rights, Europe can be a pioneer in developing business models that promote data protection and are therefore trustworthy. European companies should view this as an opportunity and a competitive advantage.

For these reasons, proposals to make the lawfulness or fundamental rights of data subjects depend on the risk associated with data processing have fortunately not found support in the European Parliament or the Council.

But the General Data Protection Regulation still contains elements of a risk-based approach, especially when it comes to technical and organizational data protection. This is not new, but is already in existing data protection law: According to Section 9 of the Federal Data Protection Act, controllers must take only those measures for which the effort involved is reasonable in relation to the purpose of protection. The General Data Protection Regulation builds on this model and lists a graduated series of elements of technical and organizational data protection based on the risks to individuals. This applies both to the individual measures to be taken, for example encryption, and to the question as to when to conduct a data protection impact assessment or when to consult the supervisory authority.

Chapter IV of the Regulation, which the Council has agreed on in principle (see No. 1.1), follows such a risk-based approach.

1.2.4 Strengthening pseudonymization

On 24 October 2014, the Federal Government sent a German note to the Council Presidency concerning the pseudonymization (as opposed to anonymization) of personal data (see No. 2.2.3).

The purpose of the paper is to increase the use of pseudonymization of personal data in order to improve protection for data subjects. The note proposed privileging the pseudonymous processing of personal data: In the case of pseudonymous data processing, the legitimate interests of data subjects would have less priority relative to the controller's legitimate interest than they would in processing not using the protection of pseudonymization. The paper also proposed anchoring the right to use an alias (pseudonym) in social networks instead of real names.

I welcome this proposal, especially since it takes up many of the ideas I suggested at expert level during the process of interministerial coordination. Moderately privileging pseudonymous data processing is certainly a feasible way to create incentives for this and other protective measures.

But a shorter and more concise definition of pseudonymization would have been desirable. The proposal contains some redundancies and is not sufficiently oriented on the existing terminology.

I also support the proposal to be able to use social networks without revealing one's own identity, although the proposed addition to recital 24 of the Regulation stating that this right may not conflict with law enforcement measures seems problematic. In the best case, this is only intended to clarify that powers provided by criminal law and the law on criminal procedures remain unaffected; in the worst case, however, it could be interpreted to mean that a database of users should be created for comparison with data from Internet access providers as a kind of data retention which would allow extensive surveillance of Internet use.

I also approve of the clear distinction between pseudonymization and anonymization. As the proposal makes perfectly clear, pseudonymized data are still personal data and are absolutely not the equivalent of anonymized data. As a result, they are covered by the scope of existing and future legislation. The note clears up the widespread misconception that pseudonymized data can no longer be traced back to a specific data subject; instead, pseudonymization represents a purely protective measure.

It remains to be seen whether these proposals will be considered, given the advanced state of negotiations in the Council of the European Union. I hope they will!

1.2.5 The future of data protection supervision

The increase of cross-border data transfers in the course of a global economy and the growing supply of goods and services via the Internet require clear procedures for businesses and – also in the meaning of citizen-friendliness - effective cooperation among the data protection authorities within the EU.

For this reason, the European Commission proposed the principle of a single contact point ("one-stop shop") in the draft General Data Protection Regulation: Businesses with multiple branches within the EU should be able to turn for assistance to the data protection authority in the member state in which their headquarters are located. This so-called lead authority would be responsible throughout the EU for all supervisory authority measures and decisions concerning the business in question; it would be required to cooperate with the competent supervisory authorities at national level. The Commission also proposed a mechanism for coordination in certain cases when multiple member states are affected by a processing operation. Known as the consistency mechanism, it is intended to bring about uniform data protection within the EU (see the 24th Activity Report, No. 2.1.1).

The one-stop shop was intensively discussed in the European Parliament and in the Council.

In its decision of March 2014, the Parliament supported the approach, proposed by the Commission, of a "lead data protection authority", but also spoke out in favour of a stronger role for the European Data Protection Board, the successor to the current Article 29 Working Party, which is supposed to be able to come to decisions in individual cases that will be binding for the competent national supervisory authority. By taking this approach, the Parliament has turned against the power the original draft of the Regulation gave the Commission to issue implementing acts to ensure the proper application of the Regulation in those cases in which more than one supervisory authority was involved in the framework of the consistency mechanism (see No. 3.1.1 on the concept of implementing acts).

The one-stop shop was also intensively discussed at Council level during the reporting period. The Lithuanian Presidency was able to bring about a substantial preliminary result at the Justice and Home Affairs Council in October 2013, where the member states approved the basic idea of a one-stop shop intended to enable the lead authority at the controller's EU headquarters to make uniform and unbureaucratic decisions in important cross-border cases.

However, the negotiations left open the question as to how far the decision-making powers of the lead authority should extend. Nor were the member states able to agree on what powers the future European Data Protection Board should have if supervisory authorities involved in a multilateral case cannot agree on how to proceed. Some member states, including Germany, thought that the Board should be able to make binding decisions concerning the application of the Regulation. Other member states argued in favour of stronger decision-making powers for the lead authority.

The negotiations also focused on how the single contact point should be designed to be as citizen-friendly as possible: Citizens are supposed to be able to take their questions and concerns to their local data protection authority and should not have to worry about questions of jurisdiction or coordination mechanisms. In the Council negotiations, this necessarily led to the question of how the different data protection authorities at the company's headquarters and at the data subjects' place of residence could come to the same decisions. In December 2013, the Council's Legal Service therefore issued an opinion proposing that the European Data Protection Board should have the power to make legally binding decisions in certain cases in which measures by local supervisory authorities would not be sufficient on their own.

Next, the Italian Council Presidency developed a model leaving the responsibility to monitor and punish violations of the Regulation and to process complaints from the public in principle to the national authorities, while requiring them in cross-border cases to work with the lead authority at the controller's EU headquarters. According to this model, not only the national authorities, but also the national courts should continue to be responsible for dealing with complaints lodged by individuals. According to the Council, and similar to the position of the European Parliament, the European Data Protection Board should act as a dispute settlement body which can make legally binding decisions if the lead authority and affected national authorities cannot agree on how to proceed.

I have been closely involved in the negotiations on the one-stop shop and the future role of the European Data Protection Board, at both national and European level. For example, at my initiative the data protection conference in March 2014 adopted a resolution on the structure of future data protection supervision in Europe (see Annex 7). In the resolution, the conference calls for the European Data Protection Board to have the power to make legally binding decisions.

During the reporting period, the Article 29 Working Party also repeatedly addressed the one-stop shop issue. At my initiative and based on the resolution of the data protection conference, the Working Party drew up a joint position paper that the Working Group's chair sent to the Greek Council Presidency in April 2014. In the paper, the Working Party also calls for a stronger role for the European Data Protection

Board which should be able to accept binding guidelines or other measures. Like the German supervisory authorities, the Article 29 Working Party also opposed EU-wide compliance procedures.

The" one-stop shop" issue has seen an overall positive development at EU level within the past two years. I believe it is crucial that the national data protection authorities should emerge stronger from the legislative process, with new procedures for cooperation and decision-making which will enable uniform and effective action in cross-border and EU-wide cases. Cooperation procedures and cooperation within the European Data Protection Board must be practical. No unreasonably bureaucratic burdens should be created for data subjects, companies or data protection authorities.

Implementing the cooperation mechanisms required by the "one-stop shop" principle will be a special challenge for Germany, with its federal division of powers. The existing structures, with 18 German data protection authorities, each having its own area of jurisdiction, will have to be reviewed by the time the General Data Protection Regulation is adopted to ensure efficient and also citizen-friendly data protection supervision. My office and I will then have to take on major new tasks in connection with the European Data Protection Board's role, which will be much larger than that of the Article 29 Working Party.

1.2.6 Transfers to third countries, Safe Harbor, impact of the Snowden affair

Cross-border flows of data and information have become routine in our globalized and interconnected world. The relevant rules in the General Data Protection Regulation build on the system and principles of the 1995 European Data Protection Directive (95/46/EC).

The General Data Protection Regulation allows data transfers from the EU to third countries when these transfers are based on decisions of the European Commission concerning the level of data protection in the recipient state, on legally binding safeguards such as binding corporate rules to protect personal data, or on standard contractual clauses. In the absence of such safeguards, data transfers may be allowed only in certain exceptional cases for certain situations defined in the Regulation. For example, data transfers to third countries may be allowed if the data subject has expressly consented to them or if they are required by contractual agreements with the data subject or by the data subject's vital interests. But the Regulation also includes rather vague conditions for exceptions, such as "important reasons of public interest" or the legitimate interests of the controller (see below).

These rules for data transfers from the EU to third countries were kept by the European Commission in its draft of the Regulation and approved by both the European Parliament in its decision of March 2014 and the Council in June 2014. After more than two years of negotiating, this was the first time the Council reached political agreement on part of the draft Regulation (including approval in principle of the so-called marketplace principle; see No. 1.2.7).

The European Parliament and the Council still see a need for revisions, among other things to the role of the European Data Protection Board, which is supposed to provide an opinion on the level of data protection in a third country before the Commission makes its decision regarding the adequacy of data protection there. The Parliament also believes that the validity of adequacy decisions already made on the basis of the 1995 European Data Protection Directive should expire five years after the new Regulation enters into force. This would also affect the European Commission's Safe Harbor decision 2000/520/EC (see also No. 4.7.1). In addition to the "classic" instruments such as binding corporate rules and standard contract clauses, data transfers from the EU to third countries based on appropriate safeguards would also be allowed on the basis of approved certification mechanisms and, in the Council's view, of approved codes of conduct as well as legally binding instruments between public authorities or bodies.

In contrast to the Commission and the Council, the European Parliament opposes allowing transfers to third countries which are not large-scale or frequent also on the basis of the legitimate interests of the controller or processor. I agree with this position. This new exception for "legitimate interests" must not become the rule for data transfers to third countries, as this would undermine the more specific data protection

instruments such as standard contracts and contractual clauses and consent of the data subject. In its opinion of September 2014, the Article 29 Working Party also emphasized that data transfers to third countries on the basis of "legitimate interests" should be the exception (see WP 222 of 17 September 2014).

The debate over protecting Union citizens' personal data from third-country government authorities was fuelled by revelations of the U.S. National Security Agency (NSA) programme PRISM in 2013 (see No. 2.1). As a result, the European Parliament called for adding a specific article to the Regulation concerning data transfers to government authorities and courts in third countries. The Parliament's proposed revision to Article 43a would make clear that the EU would neither recognize nor enforce decisions by courts and administrative authorities of a third country requiring controllers to hand over personal data unless laid down in international agreements on administrative or mutual legal assistance. In the individual case, such data transfers would require the permission of the data protection authorities and other competent authorities of the EU member states.

I agreed with this demand, which the Article 29 Working Party had already made in its March 2012 opinion on the Draft Regulation (WP 191 of 23 March 2012) and repeated in its opinion of September 2014 (WP 222 of 17 September 2014). Creating such a rule would not stop foreign intelligence services from operating in Europe, but it could create a certain amount of transparency regarding such surveillance, could help maintain proportionality and above all create incentives to conclude international agreements.

To my regret, however, the Federal Government's initiative in September 2013 to include a similar rule (here under the designation of Article 42a) in Chapter V of the Regulation was not adopted by the Council. Under what conditions third-country government authorities may gain access to Union citizens' personal data is a question which requires intensive discussion again in the upcoming negotiations between the Commission, Parliament and Council.

1.2.7 Adequacy to deal with the Internet, Big Data, profiling

I disagree with the occasionally expressed criticism that the General Data Protection Regulation is not adequate to deal with the Internet. The discussion of this issue must not lead to lower standards of data protection in the Regulation. I support the Federal Government's efforts to regulate the creation of profiles.

Along with harmonization, modernization is an explicit goal of the reform of European data protection law. The General Data Protection Regulation is intended to update the principles of data protection in effect and unchanged since 1995, when the European Data Protection Directive entered into force, in line with the digital revolution and the demands of global data traffic.

Within the Federal Government, doubts have sometimes been expressed as to whether the Regulation is adequate to deal with the Internet. Critics have said that the Regulation is insufficient to manage data protection challenges arising from cloud computing, social networks, data processing by mobile processing systems ("wearables"), Big Data analyses and extensive profiling. They say that tried and tested legal instruments such as consent and transparency rules must be questioned, while additional safeguards, or possibly even entirely new approaches, are needed.

I disagree with these criticisms. Even today phenomena such as cloud computing and Big Data can be managed and used in compliance with data protection standards, as long as strict data protection rules are followed. For example, cloud computing within the EU can be treated as third-party data processing; outside the EU, it can be governed by the rules on third-country transfers. Big Data applications could be designed to comply with the law even without requiring data subjects' consent by following the principles of purpose, necessity, data minimization, proportionality, transparency and technological data protection and using pseudonymization and anonymization. The key principles of data protection law which already exist today, such as the autonomy of the individual, transparency, purpose, relevance and necessity, can

therefore provide effective protection and ensure that data protection law remains neutral with regard to technology, which everyone wants. Such neutrality is also necessary, given the rapid pace of innovation; it would be short-sighted to try to create new data protection legislation for every new technology. The fundamental principles of data protection must therefore apply to Internet-based data processing as well.

However, the argument of inadequacy to deal with the Internet is sometimes used not because data protection law lacks safeguards, but on the contrary because it supposedly creates too many barriers. According to this argument, European data protection law is an obstacle to competition in the digital market because it does not allow EU companies to do what companies in third countries, namely leading U.S. companies, are allowed to do. I do not find this argument convincing either, for several reasons: Firstly, the marketplace principle in the Regulation means that European data protection law also applies to third-country companies which offer goods and services in the European market, thus ensuring the same conditions for competition in Europe. Secondly, European data protection law should not aspire to legitimize Big Data analyses or other data processing by reducing legal requirements, simply because such processing is technologically possible. Law should not follow technology but rather has the responsibility of setting appropriate framework conditions for technological developments. This is why I oppose a risk-based approach in which the regime of data protection law is supposed to apply only to high-risk data processing (see No. 1.2.3).

On the other hand, I agree with the Federal Government that the requirements for profiling are not yet sufficiently defined in the Regulation, even though profiling is certainly not a purely Internet-specific problem, given the many possible applications for user, behaviour, movement and other personal profiles. In particular, regulation should not be limited to the detrimental effects of a decision made on the basis of profiling; instead, regulation should start much earlier, namely with the profiling process itself. While the European Commission’s proposal only refers to measures based on profiling, which may neither be entirely automated nor have legal effects nor cause significant harm, the European Parliament’s proposal contains important improvements. But the Parliament wants the prohibition on profiling to apply only if profiling results in measures which produce legal affects for the data subject or have similarly significant effects on the interests, rights or freedoms of the data subject. The Council’s position on this issue is not yet clear. I therefore support the Federal Government’s desire to regulate profiling regardless of which requirements apply to a decision based on profiling, such as a decision not to conclude a contract.

2 Basic policy issues

2.1 The NSA scandal

2.1.1 The NSA scandal: For they know (not) what they do?

The NSA scandal has been a major focus of my activities since it broke, but no tangible results have yet been achieved. This was also due to a lack of cooperation.

As Edward Snowden revealed, U.S. and British intelligence services have intercepted, stored and analysed massive amounts of telecommunications (telephone calls, e-mails, text messages, Internet use, etc.) in the absence of specific suspicions - on a scale previously unimaginable. The surveillance also extended to persons in Germany, including holders of high political office. To investigate the matter, the German Bundestag unanimously agreed to create a parliamentary committee of inquiry, which began its work on 3 April 2014. The committee is charged with investigating not only the activities of foreign intelligence services (see Bundestag printed document 18/843 of 18 March 2014). It is also investigating whether German security authorities were involved in these activities and whether national laws or restrictions were violated or circumvented, for example whether German authorities received data from their foreign partners that they would not have been allowed to gather under German law, or whether German intelligence services collected data in Germany for foreign intelligence services which German law would not have allowed the foreign intelligence services to collect (so-called exchange of "rings" - Bundestag printed document 18/843, I.7). The committee is also looking at how the intelligence services are supervised and whether they and the ministries responsible for supervising them have met their obligations to provide information to and cooperate with regulatory bodies, including my office (with regard to the Federal Commissioner for Data Protection and Freedom of Information, see Bundestag printed document 18/843, I.12, I.17, II.5). The committee has agreed to let me, represented by my staff, participate in their meetings. This is the first time my office has been included in this way, and I welcome it. I will do my utmost to assist with the committee's investigation.

Immediately after Mr Snowden's revelations were first made public in June 2013, I asked the federal intelligence services (Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND) and the Military Counterintelligence Service (MAD), the Federal Foreign Office and the Federal Ministry of Justice for information and an explanation. Under applicable law, they are required to assist me in fulfilling my responsibilities. The information I requested was necessary among other things to prepare and carry out local inspections. Despite my repeated requests, the Federal Ministry of the Interior and the BfV refused to give me the information I asked for with a hint to my supposed lack of competence in this area. In September 2013 I submitted a formal complaint and publicly complained that these refusals were serious violations of the law. But that did not get me the information I wanted either. I do not have any further-reaching means of applying sanctions.

Despite these obstacles, I did conduct initial inspections at the BfV and BND. The inspections at the BND were especially time-consuming and labour intensive and will probably require additional time. Due to confidentiality rules I cannot provide any further details in this report. I will report my investigations and inspection results to the responsible authorities as allowed by law. I will be able to make a final assessment only after I have completed my inspections.

As soon as Mr Snowden's initial revelations became public, I offered my assistance to the parliamentary control panel and the Bundestag's G 10 Commission responsible for supervising the federal intelligence services in investigating the matter and optimizing the oversight of the intelligence services. As noted in previous activity reports (see 24th Activity Report, No. 7.7.1 ff.), there are serious shortcomings with regard to the supervision of the intelligence services and the structure of supervision required by law.

In the meantime, the Federal Ministry of the Interior conceded that, to carry out my legally mandated tasks, I may access and use personal data gathered pursuant to the Act to restrict the Privacy of Correspondence,

Posts and Telecommunications. This is an important step towards remedying these shortcomings, but by no means sufficient. Regulations and/or clarification are needed. They are yet to come. I greatly regret the fact that legislators did not adopt the necessary amendments, for example in the legislation that will make my office a supreme federal authority effective 1 January 2016.

I recommend that legislators should remedy this deficit as quickly as possible. I also call on them in particular to allocate sufficient personnel and material resources to conduct adequate inspections.

I have already referred to this in my report to the German Bundestag on surveillance activities by U.S. intelligence services in Germany (Bundestag printed document 18/59 of 15 November 2013).

My report to the German Bundestag also contains comprehensive assessments of the legal situation at national and international level, a description of existing problems and my conclusions and recommendations for action. I have referred to this public report in committee meetings, interviews, lectures and publications.

But I would like to stress here once again that the system of checks and balances for the intelligence services requires major readjustment. Especially since 2001, the tasks and powers of the security authorities have been greatly expanded, along with their personnel resources and budgets; overreaching cooperation between intelligence services and the police has been intensified at national and international level; enormous central databases have been established; and a new security structure has been created. The new national centres for cooperation between federal and state security authorities (such as the Joint Centre for Countering Extremism and Terrorism (GETZ)) serve as examples of this development.

The bodies responsible for supervision have not expanded in parallel, so there are serious legislative deficits which must be remedied as soon as possible in the citizens' interest. As the result of this development, I am no longer in a position to carry out my legally mandated tasks of advising and monitoring appropriately with the limited personnel and material resources at my disposal. So I am also no longer able to effectively perform for the citizens concerned the compensation function stressed by the Federal Constitutional Court in its decision on the Act on Setting up a Counter-Terrorism Database, that is, to determine for the persons concerned whether secret interference by the security authorities has violated their rights. According to the Federal Constitutional Court decision, such reviews are extremely important, because the persons concerned as a rule have no way of knowing about such secret interference. I urgently call on legislators to fulfil their responsibilities and create a balanced relationship between security and supervision.

This is vital to protect fundamental rights and the public trust in efficient, independent regulatory bodies, and thus for essential elements of the democratic rule of law.

I recommend to the legislator, when taking the necessary action, to consider the resolutions of the conference of the data protection commissioners of the Federal Government and of the States (Länder) of 5 September 2013 and 9 October 2014 on the unlawfulness of surveillance without just cause and on the effective supervision of the intelligence services (see annexes 6 and 11).

2.2 Big Data

The processing of larger and larger amounts of data has taken on new dimensions thanks to advances in storage technology. Today, the necessary storage capacities and computing power are available to combine and analyse massive amounts of data from a variety of sources. New ways of using these massive amounts of data, known as Big Data, in very different areas are constantly being found.

2.2.1 Big Data: Opportunities and risks

It is said that the global volume of data doubles every two years, due to the digitization of daily life and the urge to convert as much as possible into digital form. New methods and technologies are being used to develop new fields of application in connection with computing by means of large amounts of data. Both the private sector and government institutions see great potential in the use of Big Data. However, it also poses risks for the right of informational self-determination.

The most common explanation of Big Data describes it as calculating and analysing large and complex amounts of data which may also be dynamically changing. The data may be unstructured or partly structured and be a conglomeration of a variety of data collections. Advances in storage technology, computer performance, methods and algorithms make it possible to analyse such large volumes of data in close to real time.

The data come from a wide variety of sources: search queries, customer and call-related data from mobile networks, data from social networks such as Facebook, blogs and e-mails, energy consumption data from energy utilities. Data from highly diverse sources are combined in order to conduct more comprehensive and precise analyses. There are now numerous Big Data applications:

In medical research and early detection, for example, Big Data are used to try to determine which treatment is best for the patient. Analysing large amounts of data is supposed to help determine which medication is the best, with the aim of developing an individually tailored therapy for each patient.

Data centres generate comprehensive log files at various junctures. These are combined and analysed to detect anomalies, such as attacks or unlawful database queries, alterations to systems or manipulation.

Real-time analysis of search queries is a good example of a Big Data application: An unusually large number of queries in a particular region related to a hospital or flu remedy may indicate that a major outbreak of flu is on the way.

Smart meters send a flood of data to energy utilities (see 24th Activity Report, No. 10.1) which they can use to monitor and direct the flow of energy. Here, Big Data technologies can help manage fluctuations in the production of wind and solar power and offer customers individually tailored rates. But they also make it possible to keep track of what customers are doing at different times of the day, for example, as indicated by their energy use measured at brief intervals.

Big Data applications that use personal data are often incompatible with the law. They come into conflict with the fundamental data protection principles of purpose, necessity, proportionality, direct collection and transparency. Big Data processing of personal data is legal only with informed and voluntary consent of data subjects, but as a rule, obtaining consent is neither possible nor practical. This is why anonymization is crucial to Big Data applications. Given the growing collections of data from highly diverse sources, however, even the use of anonymous data poses a risk that combining data may make it possible to identify specific persons. Thus Big Data applications must be designed to ensure that no individuals are or can be identified at any stage of processing. It is not enough if the data base on which the analysis is based cannot be used to identify an individual, if, in the course of processing the data combining information with other, also de-personalized data may make it possible to identify specific persons. Especially if using highly selective criteria for analysis or a small reference group, the result of a Big Data analysis may make it possible to identify specific persons. Here, it also depends on whether third parties to whom the analysed data are sent can identify specific individuals using the existing possibilities for identification. The first example of this is the U.S. company AOL's often cited publication in 2006 of search results from its own search engine: Although the AOL user IDs had been anonymized for the search results shown and replaced with a number, the combination of the entirely unfiltered search data enabled significant and detailed personal identification, because many users had searched for information of personal interest to them,

including their own names, local addresses, familiar companies own websites, or the names of family members and friends.

Further, there is a general problem of applying anonymized analysis results to an individual. Even though Big Data analyses use anonymized data, applying the results to an individual who matches the results constitutes identification of an individual. As a result, individuals are identified if analysis results are used to determine or influence how someone is treated or judged. For example, it is standard e-commerce practice for a customer to be offered a range of payment options which depends on the likelihood that he or she will not pay. Calculating this risk is based on the anonymous analysis of a large number of previous cases. The results of this analysis are applied to the customer's available data in order to calculate the risks. Such credit scoring is naturally imprecise because it does not predict actual behaviour but only calculates probabilities – with potentially serious consequences for the individual.

Big Data will probably continue to grow even more important as additional possibilities for application and new data collections increase. Although I see great opportunities here for the private sector, Big Data applications must address compliance with data protection at an early stage and keep evaluating it anew.

In general, a regulatory framework is needed, if possible with global scope. The European General Data Protection Regulation, which is currently being negotiated, marks a first important step in this direction, as it would lead to a harmonized level of data protection not only in Europe. With its marketplace principle and the rules for transferring data, it would have an impact well beyond the European market.

Further, technological approaches are greatly needed to keep the dangers described from becoming reality. For example, smart mechanisms for anonymization or strong pseudonymization help make it possible to use Big Data technologies in a way compatible with data protection. This would also create enormous potential for innovation in the European IT industry.

Box for No. 2.2.1

Data protection requirements for Big Data:

1. In general, it is necessary to "securely" anonymize personal data at an early stage of processing; however, Big Data applications run the risk of re-identifying individuals later. So requirements of data protection law must always be kept in mind, even though the data are supposedly anonymous.

2. Using a data protection impact assessment during the design phase could help make systems protect personal data better.

3. Limiting the combination of data, reducing the length of retention, ensuring greater supervision for users:

   If the amount of available data is reduced already at the time of collection, then these data which have been "economized" are no longer available for Big Data use at a later stage.

4. Creating transparency and freedom of choice by requiring data subjects' consent.

5. Documenting responsibilities (Where do the data come from? Who collected them?).

6. Applying special safeguards to the use of especially sensitive data for purposes other than those for which they were originally collected.

2.2.2 The "Internet of Things"

Big Data is everywhere, even in this Activity Report. Global developments regarding the "Internet of Things" (IoT) are giving further impetus to data protection issues.

For a number of years now, in the private sector, especially in trade, products are being recognised by means of RFID-systems (see No. 8.6). Logistics companies use these systems to manage goods, and in manufacturing, they are used as unique identifiers for components, for example in assembling vehicles. In future, business and industry would like to expand such tracking of products and parts by enabling more and more devices to connect to the Internet in order to be able to communicate with each other. Consumers are sometimes unaware of this. The makers of these products promise that this technology will make our lives easier and more pleasant, for example with regard to motor vehicles or health care. Because of the topicality of this issue, the International Conference of Data Protection and Privacy Commissioners addressed it in 2014 (see No. 4.3 and the box below).

Many products already contain data sources for Big Data and the Internet of Things, as the following examples show:

A modern television set is practically a computer with a large monitor; a video game console is a complete media centre in a child's bedroom; and a fitness wristband combined with a smartphone is a data centre with very personal information about its user. One wonders whether it is possible to use these new technologies of the entertainment industry without worrying.

With the new video game consoles, protecting children's personal data has become a concern: The latest generation of devices has sensors, cameras and technologies to recognize different players and their movements or to respond to commands by gestures or spoken key words. Users can hardly control what the device records about them. A console constantly registers all kinds of personal information about its user: reaction times, learning capacity or emotional states. This information can then be processed on an external server and possibly even sent to third parties. The data subject has little control over whether this information is ever deleted.

In some cases, all it takes to active the system is a spoken keyword. So users worry that everything they say could be stored and analysed, with the console acting as a "bug". I think it is unlikely that device manufacturers will abuse the microphone surveillance feature, as some fear, but hackers could be a potential threat by taking advantage of vulnerabilities when data are sent over the Internet. On some models, the console itself conducts facial recognition: The camera is able to recognize users' emotions or the number of persons in a room. This is valuable information for advertisers and market researchers. Ultimately, one must trust that the manufacturer will not secretly collect data and will obey the rules of data protection.

Modern TVs too now have the potential to spy on their owners. In the 1990s, television sets were not yet "smart" or connected to a network. Since then, living rooms have become "wired", with all kinds of devices, such as BluRay players, hard drives, tablets, game consoles and smart TVs connected via Wi-Fi routers. The Internet has moved from the classic desktop computer into all sorts of terminal devices.

With the help of the new smart receivers with hard drives or smart TVs, not only can users access all kinds of media formats, they can also view various additional information on hybrid broadcast broadband TV (HbbTV), the successor to teletext. HbbTV delivers prepared information from TV broadcasters and their media libraries via the Internet. This is a wonderful thing in theory, but it means that the TV set also sends large amounts of data back to the Internet, possibly enabling users to be identified. This is all the easier if the TV set also transmits a unique device identifier. So third parties may be able to find out what you are watching at any given time, and they might be able to combine these data with other data, such as user profiles from other Internet services.

Another current trend is fitness wristbands which record and monitor movement and health data such as heart rates and movement during sleep. All the data are accessed using a smartphone or PC and often stored in the manufacturer's cloud. The new generation of mobile telephones also has sensors which use special applications to collect data about us. With the help of built-in position tracking, this information is then combined with spatial data, making it possible to create highly personalized movement and health profiles. In this way, your mobile phone becomes the hub of all your activities and thus also a data centre. New devices such as smartwatches will further advance this trend. Health insurers have found an opening in the market and are already giving customers free fitness wristbands to test whether they can help in detecting illnesses. Special caution is required above all when it comes to health information: You should never give third parties any information which could be used to create health profiles or indicate the existence of illnesses. Who knows whether these data could work to your disadvantage in future (see No. 13.1)?

Various manufacturers and financial institutions are in the process of testing or introducing the option of mobile payment using near field communication (NFC). The electronic wallet could soon supplement or even replace other methods of payment. At the moment, however, only newer and more expensive mobile devices have the necessary chip. With all of the electronic devices of entertainment referred to here as examples, there is a risk that personal profiles will be created and data protection law violated. For this reason, the various working groups of the Düsseldorfer Kreis and the conference of data protection commissioners have to keep on top of the latest trends. It remains to be seen what new technologies we will face in the future and whether all these new technologies and devices will succeed in the market despite data protection concerns.

Box for No. 2.2.2

The 36th International Conference of Data Protection and Privacy Commissioners on 13–14 October 2014 (see No. 4.3) prepared a declaration on the Internet of Things recognizing self-determination as an inalienable right for all human beings (available on my website at www.datenschutz.bund.de). The Internet of Things increases the risk either that businesses and authorities will acquire personal information about us, or that we will adapt our behaviour accordingly. Both interfere with the right of informational self-determination. The conference therefore made the following recommendations:

- The quantity, quality, timeliness and sensitivity of data collected by the Internet of Things will continue to grow. Such data should therefore be regarded as personal data.

- Business models based on the Internet of Things must be sufficiently transparent and explain which services are accessing which data.

- Ubiquitous computing (see 23rd Activity Report, No. 1.5) will continue to grow in importance, making possibilities for anonymous use and obligations to minimize the data collected (Section 3a of the Federal Data Protection Act) ever more important as well.

- Consumers' privacy must be protected from the outset using Privacy by Design, Privacy by Default and the like. Data protection and security should be regarded as key selling points.

- The Internet of Things also poses significant challenges to IT security. To minimize the risks associated with the Internet of Things, end-to-end security is needed not only for communication between individuals (such as e-mail), but also for communication between devices, for example to protect against eavesdropping by other smart devices.

- Data protection legislation and the EU's new General Data Protection Regulation must be able to deal with the demands arising from Internet of Things technologies.

A subgroup of the Technology Subgroup has also published a paper on the Internet of Things (see No. 3.1.4). The International Conference also adopted a resolution on Big Data (also available in English on my website, www.datenschutz.bund.de).

2.2.3 Effective anonymization and pseudonymization, please!

Privacy-enhancing technologies are an important tool for protecting personal data and achieving classic data protection aims. But these measures must be effective and possible residual risks taken into account. This also applies to the anonymization and pseudonymization of personal data.

In an era of massive amounts of data (see No. 2.2), protecting personal data is increasingly important. In particular publicly accessible data, known as "open data", offer enormous potential, whether for research purposes or because they are available free of charge. But if data can be traced to a specific individual, publishing them or making them available to others can be problematic in terms of data protection law.

In addition to the technical and organizational measures pursuant to Section 9 of the Federal Data Protection Act, anonymizing and pseudonymizing personal data are effective ways to protect them. But the two processes are often confused with each other, intentionally or unintentionally.

The difference between anonymization and pseudonymization

The Federal Data Protection Act defines anonymization as altering personal data in such a way that information concerning personal or material circumstances can no longer be traced to an identified or identifiable natural person without unreasonable effort (see Box A below). This definition refers to both absolute anonymization and anonymization in fact. The latter is the case when data can be traced to a specific person only with disproportionate effort. Anonymized data are not covered by national or European data protection legislation.

By contrast, pseudonymization involves replacing the identifying features of datasets with other identifiers (pseudonyms) (see Box A below). Pseudonymization represents a useful protective measure, because it may be desirable to retain some connection between the original and the pseudonymized data (for example, to report research results to data subjects), though this should be allowed only under strict conditions and for a limited group of people. But pseudonymization is not the same as anonymization. Pseudonymized data are still personal data and are covered by national and European data protection law.

Effectiveness of anonymization

As early as 1997, Germany's data protection commissioners of the Federal government and of the States (Länder) addressed the quality of anonymization techniques in their working paper on data protection-friendly technologies (17th Activity Report, No. 8.5), stating that the highest level of anonymity is ensured when personal data are not generated in the first place. Because this is not always possible, it is urgently necessary to define criteria for effective anonymization and for avoiding residual risks of re-identification.

Anonymization procedures should always be based on established, state-of-the-art processes and algorithms. Procedures developed in-house often have serious shortcomings. Data should be deleted when the purpose for which they were stored no longer applies - this is true in other contexts as well-. Procedures for anonymization should be taken into consideration already during the development phase (see "Privacy by Design" and "Privacy by Default", 23rd Activity Report, No. 3.1) and implemented at an early stage.

In its opinion on anonymization techniques (WP 216 of 10 April 2014; see also No. 3.1.4 in this report), the Article 29 Working Party tested the robustness of each technique based on three criteria:

- Singling out: The possibility to isolate some or all records which identify an individual in the dataset;

- Linkability: The ability to link, at least, two records concerning the same data subject or a group of data subjects;

- Inference: The possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

According to the Article 29 Working Party, only those solutions offering protection against all three of these risks are able to rule out the possibility of re-identification (see Box b for No. 2.2.3).

Use of pseudonymization

In its opinion, the Article 29 Working Party also cleared up the misconception that pseudonymization is a technique for anonymization, thereby contradicting certain interest groups who would like to define pseudonymized data as a separate class of personal data.

Pseudonymization precisely does not meet the three criteria for effective anonymization.

But pseudonymization may make sense when anonymizing data is out of the question. For pseudonymization to be effective, similar principles apply as to anonymization. In addition, it is necessary to ensure that data can be re-identified only under strict conditions and for a very limited group of people. In its opinion, the Article 29 Working Party listed vulnerabilities and common errors in this regard.

Pseudonymization, anonymization within the framework of the reform of European data protection law

In the context of the negotiations on the General Data Protection Regulation, the Federal Government sent the Council Presidency a note concerning pseudonymization and anonymization, most of which I agree with (see No. 1.2.4). The note proposes privileging the processing of pseudonymized data under certain conditions.

Box a for No. 2.2.3

Federal Data Protection Act, Section 3: Further definitions

[…]

(6) Anonymization means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.

(6a) Pseudonymization means replacing a person’s name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.

[…]

Box b for No. 2.2.3

Example:

A federal institute has a database on an extremely rare disease. The data are anonymized so that only the data subjects' city or town of residence is stored. So it is initially almost impossible to identify individuals.

Over time, however, additional content about the individual data subjects is added: when they had a cold or an accident; later, additional illnesses are added, etc. In individual cases, it is now possible to identify a specific person, especially if he or she lives in a small community.

In this case, the data have *not* been anonymized, because the addition of further data makes it possible to link records (risk: Linkability) relating to an individual, to single out (risk: Singling out) an individual and thus to re-identify a specific person.

2.3 Decisions by the European Court of Justice

The European Court of Justice delighted or shocked – depending on one's perspective relating to data protection law – the data protection community within a single month with two decisions: While its ruling on data retention did not surprise the experts, its decision on the obligations of search engine operators came like a thunderclap. With both decisions, the European Court of Justice underscored the importance of fundamental rights of data protection.

2.3.1 The end of data retention?

The European Court of Justice found that the Data Retention Directive violated European law and declared it to be null and void, even retroactively.

The issue of data retention has been dealt with repeatedly in previous activity reports (most recently in the 24th Activity Report, No. 6.1 and the box for No. 6.2). After Germany's Federal Constitutional Court declared the act implementing the Data Retention Directive (2006/24) to be invalid (judgment of 2 March 2010), the European Court of Justice also found that the violations of fundamental rights in the EU Data Retention Directive made it null and void (judgment of 8 April 2014, file ref. C-293/12 and C-594/12). The court found that the serious and disproportionate interference with the fundamental rights to respect for private life and the protection of personal data caused by the Directive violated Article 7 and Article 8 of the EU Charter of Fundamental Rights. In particular, the court criticized the Directive's insufficient rules and lack of specificity, stating that especially in view of the far-reaching impacts and the informative value resulting from the comprehensive surveillance of the communications of practically the entire European population, the EU legislation should have specified clearer and more precise rules. Only in this way would it be possible to ensure that the measures called for in the Directive were proportionate and limited interference with fundamental rights to what is strictly necessary.

Above all, the judges in Luxembourg criticized the fact that the Directive was intended to fight serious crime but was not at all limited to the persons or data needed to actually pursue this goal. Instead, the court found that it justified storing all communications, including those of persons whose communications are subject to the obligation of professional secrecy.

The court also found that the Directive did neither lay down any objective criteria to limit the number of persons authorized to access and subsequently use the data retained, nor did it make access to the data retained depend on a prior review carried out by an independent administrative body or a court.

Further, the court found that the retention period of 6 to 24 months had been set without providing objective criteria to ensure that it was limited to what is strictly necessary.

And the court found that the Directive did not require the data in question to be retained within the European Union and that independent data protection supervision, which is explicitly required by the Charter of Fundamental Rights, could not be fully ensured.

As a result of this judgment, there is no longer a legal basis for data retention within the area covered by European law.

However, many officials responsible for interior and security policy as well as law enforcement representatives continue to argue that data retention is crucial in order to fight crime effectively and that new national legislation is needed. But at the time this report went to press, no answer was yet forthcoming as to how such national law would be able to satisfy the demands of the European Court of Justice. In particular, the question of how to limit data retention only to communication that is in fact relevant, which conflicts with the principles of comprehensive and groundless data retention, remains unanswered.

The European Commission has announced that it will thoroughly review the judgment before assessing its impacts with the participation of all stakeholders. As a result, it is not yet clear whether there will be a new initiative for a directive on data retention at European level.

It remains to be seen whether the European Court of Justice judgment spells the end of data retention, but the shortcomings found by the court have clearly shown that this form of data retention is not compatible with the protection of fundamental rights.

2.3.2 New obligations for operators of search engines

In its ground-breaking judgment of 13 May 2014 (C-131/12), the European Court of Justice found that search engine operators such as Google are responsible under data protection law for the publication of search results, and that under certain conditions they must remove links from the list of search results at the request of users affected.

Probably very few expected this result from the court in Luxembourg: In the key issue, the judgment departed not only from the final motion of the Advocate General, which the judges typically follow, but also from the position of the Article 29 Working Party, which had almost unanimously argued that search engine operators were not responsible for processing personal data published on a third-party website displayed as a link in their lists of search results. In its 2008 opinion on data protection issues related to search engines (WP 148 of 4 April 2008), the Article 29 Working Party left open whether search engine operators are responsible for the search results displayed only in order to include the rules already issued by one member state on removing content data from the list of search results.

The European Court of Justice judgment in the Google case has led to new perspectives and legal certainty in a number of highly relevant questions of interpretation: Almost as an aside the court said that enterprises intended to promote and sell advertising space on search engine results pages are to be regarded as “establishments”, justifying the application of European data protection law to third-country providers, such as U.S. companies like Google. Because according to Directive 95/46/EC, European law also applies to companies outside the EU if the “processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State”. The European Court of Justice found that this context exists if the establishment provides financial support for the data processing.

Having even greater significance and broader implications is the court’s statement that, by using indexing programmes to retrieve, record and organize data which it stores on its servers and discloses and makes available to its users in the form of lists of search results, search engine operators independently process personal data and are therefore responsible under data protection law.

The resulting obligation of search engine operators to remove, under certain conditions, links to websites with information about persons affected is rightly seen as significantly reinforcing data protection.

However, it has also been criticized as endangering the freedom of the press and of expression. According to these critics, the court focused too much on the interests of the data subjects while neglecting the interest of the general public in using search engines and that of website operators, who rely on search engines for their audience and whose freedom of expression and freedom of the press could be harmed. They also argued that if in case of doubt, search engine operators such as Google responded to the anticipated flood of de-listing requests by deleting links, the ability of search engines to function would ultimately be limited, interfering with the ability to find Internet content. So it is certainly appropriate to speak of "the right not to be found", rather than "the right to deletion", because the court did not require taking down the original website but only removing the link to it.

In their resolution of 9 October 2014, the data protection commissioners of the Federal government and of the States (Länder) welcomed the court's judgment and called for its effective implementation (see No. 1.2.2 and Annex 10). The Article 29 Working Party stressed the need for a uniform European response. After intensive discussions, in late 2014 it published guidelines for implementing the judgment. In addition to a summary evaluating the judgment and the resulting requirements for its implementation in practice, the guidelines include assessment criteria intended to ensure uniform practice by data protection authorities when handling complaints about de-listing requests that have been rejected by search engine operators.

For a request for removal from a list of search engine results to be considered legitimate, the search engine must display the link in question as the result of a search for the name of the data subject submitting the request. If this condition is met, the request is then checked to see whether the information on the website in question is accurate, subject to special protection or out of date; whether it is offensive or defamatory; and whether it would give the data subject reason to fear negative consequences or special threats. With regard to the interest of Internet users in information, it is also necessary to consider whether the data subject is a public figure and whether the information was published for journalistic purposes. The data protection authority decides based on the facts and after weighing the various interests; a single factor on its own can never be the deciding factor.

The catalogue of criteria should not be regarded as conclusive and can be expanded as additional practical experience is acquired. No information on cases was available at the time this report went to press. The guidelines may be accessed on my website, www.datenschutz.bund.de

2.4 Data protection supervision now independent also at federal level

The German Bundestag passed legislation on 18 December 2014 making the office of the Federal Commissioner for Data Protection and Freedom of Information an independent supreme federal authority subject only to parliamentary and court supervision.

Since this office was established in 1978, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) has been located within the Federal Ministry of the Interior. Although according to the Federal Data Protection Act the BfDI is independent, it is subject to the legal supervision of the Federal Government and the administrative supervision of the Federal Ministry of the Interior. BfDI staff are employees of that ministry, which is the supreme authority, and the Federal Minister of the Interior is the superior with ultimate responsibility for personnel matters.

This organizational structure and the legal status of the BfDI do not comply with European law as expressed in the 1995 European Data Protection Directive (95/46/EC), which requires member states to set up supervisory authorities which are "completely independent" in performing their assigned duties.

The European Court of Justice further specified the interpretation of "complete independence" in three judgments concerning Germany (2010), Austria (2012) and Hungary (2014). Although the Federal Government argued that the 2010 judgment applied only to data protection supervision in the private sector at state level (see 23rd Activity Report, No. 2.1), the 2012 judgment concerning the independence of Austria's data protection authority made it clear that the legal status of my office did not comply with

European law either, as the Austrian case was very similar to the legal situation in Germany under the Federal Data Protection Act (see 24th Activity Report, No. 3.1).

The Federal Government finally realized the need to take legislative action, as I had been requesting for years, and presented a bill to that effect in summer 2014. After the Bundesrat was consulted and the Bundestag Committee on Internal Affairs held a public hearing of experts, the legislation was adopted by the Bundestag plenary on 18 December 2014 and is supposed to enter into force on 1 January 2016.

Under the new law, my office will become completely independent of the Federal Ministry of the Interior; the Federal Government will no longer be responsible for its legal supervision, nor the Federal Ministry of the Interior for administrative supervision. My office will be a new government agency with the status of a supreme federal authority, subject only to oversight by the German Bundestag, and my decisions will of course be subject to review by the courts.

In this way, Germany will fulfil the essential minimum requirements of European law. But I had hoped for more.

For example, I had suggested, among other things, that the new law should also provide for cooperation and staff exchanges with all federal ministries and other supreme federal authorities. The BfDI will be by far the smallest supreme federal authority and will have no executive agencies, so it will have to recruit some qualified and experienced staff from other government agencies. It would therefore be important for staff to be able to transfer to and from other supreme federal authorities. I am currently negotiating an agreement to this effect with the Federal Ministry of the Interior. If the provision I suggested had been included in the law, such an agreement with other supreme federal authorities could have been made on a secure legal basis.

To ensure legal certainty for the future structure as a supreme federal authority, I had also proposed providing in the law for the possibility of setting up field offices, analogous to Section 2 (1) of the Federal Audit Office Act (BRHG).

A provision which would have made my testimony in court and before parliamentary committees of inquiry partly depend on the consent of the Federal Government and thereby still subject to executive approval was dropped after contentious political debate. Almost all the experts at the German Bundestag's public hearing on 1 December 2014 spoke out against this provision, as did I, because it would have constituted unreasonable interference with my independence which would have been problematic under European law. The new law now makes clear that I am only obligated to consult the Federal Government in cases which could affect the core area of its executive responsibility.

My office also needs greater powers to take action and issue sanctions, especially in the area of posts and telecommunications. If providers of postal or telecommunications services violate data protection provisions of the Postal Act or the Telecommunications Act, the only action I can now take is to submit a complaint to the Federal Network Agency (Bundesnetzagentur). Nor do I have the authority in this area to levy fines in case of violations of the Federal Data Protection Act. As a result, violations often go unpunished (see 24th Activity Report, No. 6.9 with further references). By contrast, my counterparts in the federal states have effective powers to issue orders and prohibitions in every other area of the private sector; most are also authorized to prosecute civil infractions and levy fines. Parity between the federal and state levels is urgently needed in this regard. During the legislative process, I therefore insisted that this issue should be addressed as soon as possible with new or amended legislation, so that the effective powers of intervention required by European law are finally created also in the area of postal services and telecommunications.

But independent data protection supervision requires more than just organizational autonomy, which does not bring about the desired effect if it is not accompanied by the capacities and possibilities to ensure

independent oversight. I can perform my duty as protector of the fundamental right to privacy in complete independence only if I have the necessary resources at my disposal.

The much-discussed draft of the EU's General Data Protection Regulation rightly considers providing data protection authorities with the resources necessary to perform their tasks to be one element of the complete independence of data protection supervision.

Germany's new law on the BfDI does not meet these requirements. It does neither draw the necessary conclusions from the organizational independence of the BfDI, nor does it address the existing under-provision of resources, which is an even more serious problem. Particularly, but not only, in the crucial area of monitoring the intelligence services, the human resources necessary to ensure the intensity of inspections which the Federal Constitutional Court believes is urgently required have been lacking for years (see also No. 5.2).

I can only hope that, in its budget debates, the Parliament will declare its support for effective data protection and will thus improve the protection of the citizens' fundamental rights. Thanks to my being appointed by the German Bundestag, to my close cooperation with the Parliament and the fact that my office will soon be organizationally independent from the Federal Government, as a supervisory body I will in future be more closely associated with the Parliament. I therefore hope that the German Bundestag will be more willing to provide "its" data protection authority with the necessary resources to perform its tasks.

4 Committee on Foreign Affairs / Committee on the Affairs of the European Union / Committee on Human Rights and Humanitarian Aid

4.1 International data protection - Article 17 ICCPR

National or European regulatory initiatives are not sufficient to address the ongoing globalization of data flows. I have therefore been advocating the strengthening of privacy rights also at the level of international law.

As clearly demonstrated by Edward Snowden's 2013 revelations of government surveillance and by the explosive growth of globally accessible data, national or regional approaches to protect these data have only limited effect.

For this reason, I welcomed the Federal Government's announcement, in its eight-point programme, that it would support an additional protocol to Article 17 of the UN's International Covenant on Civil and Political Rights (ICCPR) to improve privacy protection at international level.

Unfortunately, the Federal Government's proposal to convene a conference of parties to the ICCPR found few supporters. The Federal Government (Federal Foreign Office) also pointed out to me that UN-level initiatives to improve privacy protection run the risk of being watered down, ultimately resulting in weaker protection.

The German-Brazilian initiative for a General Assembly resolution (A/C.3/68/L.45) on the right to privacy and charging the UN High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic and extraterritorial surveillance was much more successful (see No. 4.3). In her report published in June 2014 (A/HRC/27/37), the High Commissioner refers to existing international law provisions, such as Article 17 of the ICCPR, but finds shortcomings with regard to the implementation of the provisions into national regulations and insufficiency as regards supervision. She recommends that states should review their own national laws, policies and practices to ensure full conformity with international human rights law and calls for a dialogue involving all interested stakeholders.

The 36th International Conference of Data Protection and Privacy Commissioners, which was held in Mauritius from 13 to 16 October 2014, addressed this opportunity for a multi-stakeholder dialogue on data protection in the context of modern communications technology with a resolution I supported (available in English on my website, www.datenschutz.bund.de, and at www.privacyconference2014.org). The 35th International Conference in Warsaw in September 2013 had already expressed its support for an additional protocol to Article 17 ICCPR, to be based on the International Standards on the Protection of Data and Privacy (Madrid Declaration) adopted by the International Conference in 2009 (see No 4.3; available on my website, www.datenschutz.bund.de).

It is a good sign that the Federal Government is continuing its efforts to improve the protection of privacy at international level. This is proven by Resolution A/C.3/69/L.26, which Germany and Brazil again introduced in late 2014 and which is available at the United Nations' website www.un.org.

I fully support the German-Brazilian initiative to designate a special rapporteur for the debate over the right to privacy in the digital age.

4.2 Conference of European Data Protection Authorities

In 2013 and 2014, the annual Spring Conference of European data protection commissioners focused above all on the future of data protection in Europe.

The Conference of European Data Protection Authorities, in which data protection authorities from Europe participate along with representatives of the European Commission, Council of Europe and the OECD, is traditionally held in April or May every year and is thus known as the "Spring Conference", to distinguish it from the International Conference of Data Protection and Privacy Commissioners, which regularly takes place in autumn (see No. 4.3 below). The Spring Conference offers a forum for sharing ideas and experience among all the data protection authorities in Europe; it thus includes not only those within the EU, but also data protection commissioners from Council of Europe countries, in particular the countries of south-eastern Europe.

The Portuguese data protection authority hosted the 2013 Spring Conference, which took place in Lisbon on 16 and 17 May. Conference participants discussed the future of data protection in Europe and adopted a resolution in which the European data protection commissioners stressed that the reform of EU data protection legislation and the update of the Council of Europe data protection convention, which are both currently under way, must be coordinated in order to avoid any contradictory evaluation later on. The Spring Conference also adopted resolutions on ensuring appropriate data protection at Europol and on safeguarding data protection in a transatlantic free-trade zone, which the Conference participants consider crucial (on TTIP, see No. 8.7).

The Council of Europe and the French data protection authority CNIL co-hosted the Spring Conference in Strasbourg on 5 June 2014. The central topic was improving Europe-wide cooperation among data protection supervisory authorities, especially with regard to multinational or globally active enterprises. With this in mind, the Conference established a working group to draft proposals in time for the next Spring Conference. I support their activity because I believe cooperation among the supervisory authorities is absolutely essential to perform the assigned tasks effectively (see No. 4.4). The Conference also adopted a resolution on updating the Council of Europe convention on data protection. The resolution calls on the Council of Europe member states to maintain a high level of data protection even if non-member states plan to accede to the convention.

The text of the resolutions adopted at the 2013 and 2014 Spring Conferences is available on my website, www.datenschutz.bund.de.

The next Spring Conference will be held in Manchester in May 2015, hosted by the British data protection authority.

4.3 International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners addressed key issues of the future and adopted initiatives to improve global cooperation.

After two meetings in Latin America (in Mexico in 2011 and Uruguay in 2012), the International Conference of Data Protection and Privacy Commissioners returned to Europe in 2013: The 35th International Conference of Data Protection and Privacy Commissioners was hosted by the Polish data protection commissioner in Warsaw on 23–26 September 2013. Under the heading "Privacy: A Compass in a Turbulent World", the Conference took on the task of offering orientation for users and stakeholders in world that is more and more complex, with new and increasingly data-intensive applications and services.

During the closed session, which is reserved for data protection commissioners and their deputies, the Conference focused on the "appification" of society: the fact that small software applications ("apps") are constantly being developed for new purposes and situations, especially for mobile devices (smartphones and tablets) and offered to consumers, often free of charge. To use these apps, however, consumers usually have to allow the application to access the data on their mobile device, often including the user's location data and thereby enabling the creation of movement profiles. For this reason, in its Warsaw Declaration on the "appification" of society, the 35th International Conference said that the principles of data protection, such as purpose limitation, necessity and data minimization, must apply to these innovative applications

too, and that users need sufficient transparency about which of their data are collected and how they are processed.

As further aids to orientation, the Conference also adopted resolutions on profiling, web tracking and digital education (all resolutions available on my website, www.datenschutz.bund.de).

At the initiative of my office and with support from data protection authorities in Europe, Asia and America, the 35th International Conference adopted a resolution on anchoring data protection in international law and called on governments worldwide to advocate a binding international agreement on data protection. To do so, the resolution proposes building on Article 17 of the ICCPR covering the protection of the home and privacy and on the International Standards on the Protection of Data and Privacy adopted by the International Conference in 2009 (see also No. 4.1).

In 2014, the International Conference met for the first time in Africa, where the data protection authority of the Republic of Mauritius hosted the event on 13–16 October.

The closed session focused on the Internet of Things (see also No. 2.2). Advances in miniaturization technology have made it possible to incorporate sensors into smaller and smaller devices which are able to constantly gather data. One example is fitness wristbands which constantly record the wearer's heart rate and number of steps taken and transmit this information to a mobile device such as a smartphone or tablet, where it can be further processed using a health app. This continuous collection and storage of personal data enables the creation of extremely detailed individual user profiles which can reveal a great deal of information, including sensitive information, about the wearer, especially if Big Data analyses are used. The Mauritius Declaration on the Internet of Things therefore calls for greater protection for users' data, for example by making use of anonymized data. In particular the use of data for purposes other than those for which they were originally collected and transfer of data to third parties ("out-of-context use") should be strictly regulated. And when purchasing an Internet of Things device, consumers should be informed about how it will process their data.

The resolution on Big Data, which I co-sponsored along with the resolution on the right to privacy in the digital age, should also been seen in this context. The latter refers to the UN General Assembly's resolution of December 2013 on the same issue, which was adopted at the initiative of Germany and Brazil in the wake of the mass surveillance programmes run by certain governments and revealed in summer 2013 (see No. 4.1).

The International Conference also adopted a resolution on increasing cross-border cooperation among data protection supervisory authorities and approved a related cooperation agreement (all resolutions are available in English at www.privacyconference2014.org and on my website, www.datenschutz-bund.de).

The 37th International Conference of Data Protection and Privacy Commissioners will take place in Amsterdam from 26 to 29 October 2015.

4.4 Improved cooperation among the European data protection authorities

Proven instruments and new initiatives have strengthened and deepened cooperation among the data protection authorities in Europe.

Spring Conference Working Group on European Cooperation

In spring 2014, the Conference of European Data Protection Authorities established a new working group intended to improve cooperation among the European supervisory authorities beyond those in the EU member states (see also No. 4.2). The Working Group is co-chaired by the French data protection authority CNIL and the Council of Europe's Ad hoc Committee on Data Protection (CAHDATA). The Working

Group's results are to be presented at the Spring Conference in 2015. Because I believe that cross-border cooperation among data protection authorities is absolutely essential to ensure effective supervision, I support the establishment of the Working Group and am participating in its activities.

Case-handling workshops

As in previous years, case-handling workshops were again offered during the reporting period under the aegis of the Conference of European Data Protection Authorities: in Sarajevo (Bosnia-Herzegovina) in October 2013, and in Skopje, former Yugoslav Republic of Macedonia, in October 2014. The workshop format has proved useful for sharing experience and knowledge among the European data protection authorities. The workshops are intended to encourage consistent and uniform practice to ensure that data protection authorities achieve similar solutions to similar problems of data protection. Staff of newer data protection authorities in particular can benefit from the others' experience and familiarize themselves with specific, practical problems and questions that arise in daily practice. I support the model of case-handling workshops, because sharing experience and helping other data protection authorities in Europe is very important to me.

European administrative assistance

The European Commission's Technical Assistance and Information Exchange (TAIEX) has proved useful in helping data protection authorities in the candidate countries for accession to the EU, providing tailored assistance and support in individual cases. As in previous years, during the reporting period I assisted various data protection authorities, especially in south-eastern Europe. For example, I participated in expert missions in Montenegro and the former Yugoslav Republic of Macedonia and hosted visiting delegations from the data protection authorities of the Republic of Moldova and Albania at my office.

I also advised the office of the Ukrainian parliament's ombudsperson for human rights, which in early 2013 assumed the function of a data protection supervisory authority in Ukraine. I would like to thank the German Foundation for International Legal Cooperation (IRZ) in Bonn for its helpful assistance in this context.

New European Data Protection Supervisor

The first European Data Protection Supervisor (EDPS), Peter Hustinx, left office in late 2014; his term had already expired in January 2014, but he continued as acting EDPS until a successor was appointed. I would like to thank Mr Hustinx for his tireless efforts on behalf of privacy as an inalienable fundamental right in Europe and the world. I would also like to congratulate Giovanni Buttarelli, the former deputy EDPS, on his appointment as the new European Data Protection Supervisor. I look forward to working together productively and on the basis of mutual trust.

4.5 OECD: Working Party on Security and Privacy in the Digital Economy

Following intensive preparations by its Working Party on Security and Privacy in the Digital Economy (SPDE), the OECD adopted revised guidelines on the protection of privacy in summer 2013. The Working Party is currently updating the guidelines on data security.

During the reporting period, the Working Party on Information Security and Privacy, (WPISP) of the Organization for Economic Cooperation and Development (OECD) worked on finishing the OECD Privacy Guidelines (see also 24th Activity Report, No. 2.4.5). Following intensive discussions within an expert group, whose efforts I also contributed to, it was decided to retain the eight existing data protection principles, including transparency and purpose limitation in data processing. New additions are privacy management programmes which businesses must use to provide their customers and the authorities with information relevant for privacy protection. The new guidelines also call for data breach notification in case

of violations of data security or data protection and stress the importance of international cooperation in view of growing global flows of data.

In early 2014, WPISP was renamed the Working Party on Security and Privacy in the Digital Economy (SPDE). In line with the mandate expressed in its new name, the SPDE is concerned not only with protecting privacy, but also with ensuring the security of personal data. With this in mind, the OECD's 2002 guidelines on data security are currently being updated to reflect the growing economic and societal importance of the Internet in OECD member states as well as new technological developments such as cloud computing and the Internet of Things. The updated guidelines on data security are to be adopted by the end of 2015.

4.6 Council of Europe: A modern foundation for data protection law in Europe

The efforts to update the Council of Europe Convention 108 are making good progress. The Convention on the Manipulation of Sports Competitions could be more data-protection friendly.

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, is long overdue for updating, given the many technological innovations in the field of data processing over the past 30 years (see also 24th Activity Report, No. 2.4.5). But it has not yet been possible to finish revising the Convention while the negotiations on the EU's General Data Protection Regulation (see No. 1) are still going on, because a major goal of modernizing the convention is to largely harmonize the regulatory frameworks of the Council of Europe and the EU.

From the negotiations, improvements to the Convention are already apparent, which I am very pleased about. Of special note are the expansion of the Convention's scope to include manual data processing, the explicit mention of especially sensitive personal data such as biometric and genetic information, and (under certain conditions) the opening of the Convention to non-member states of the EU and the Council of Europe. The last-mentioned in particular leads to hopes that European data protection values could receive more attention also beyond Europe in future.

Unfortunately, I cannot directly participate in the negotiations on modernizing Convention 108 but can only be heard indirectly through my cooperation with the Federal Ministry of the Interior, which represents Germany in the working party. In its resolution of 5 June 2014, the Conference of European Data Protection Authorities called for direct participation by the national data protection authorities.

The Committee of Ministers of the Council of Europe also adopted the Convention on the Manipulation of Sports Competitions, which was signed by the sport ministers of the Council of Europe member states on 18 September 2014. In participating through the lead Federal Ministry of the Interior, I made proposals to better anchor data protection in the Convention.

4.7 International data protection: Individual issues

Along with special issues of participation in international organizations and bodies, during the reporting period I focused on various individual issues of data protection at international level:

As in previous years, I carefully followed the trends in data protection in the U.S. (see No. 4.7.1).

New developments, which some of my European counterparts and I supported, have resulted from the efforts of the EU and APEC to compare certain data protection rules from each of their areas of application (see No. 4.7.2).

And I kept an eye on the issue of how passenger name records are used, especially by the security authorities, in Europe and other parts of the world (see No. 4.7.3).

4.7.1 Trends in U.S. data protection law

Despite some encouraging signs, the development of data protection law in the U.S. stagnated during the reporting period. Massive surveillance without reasonable suspicion by the U.S. intelligence services threatens the rules on data transfers between the U.S. and Europe.

In his state of the nation speech in February 2013, President Barack Obama gave reason to hope for greater attention to data protection in the U.S. when he stressed the value of protecting privacy. In May 2014, the Podesta Report addressed the impact of Big Data and gave the U.S. government numerous recommendations for improving data protection, including a call for legislation on data breaches and recommendations that U.S. law on privacy protection should also cover non-U.S. citizens and that the Consumer Privacy Bill of Rights should be expanded.

Unfortunately, no action has been taken beyond these announcements. Neither the Consumer Privacy Bill of Rights, presented in 2012 (see 24th Activity Report, No. 2.5.4) nor the recommendations in the Podesta Report have led to any legislative proposals.

On 25 April 2014, a New York district court ruled that Microsoft was required to give an unspecified U.S. government agency information about a customer's e-mail account (see No. 9.3.2). This decision has special relevance, because the search warrant and confiscation order also cover data stored on servers in the EU, in this case in Ireland. The court found that U.S. law applied also to these data simply because a company with headquarters in the U.S. was involved. This extremely broad interpretation of the scope of U.S. law which completely ignores the regulatory framework for data protection in Europe is one reason for concern; another is the fact that international mutual legal assistance treaties intended for such cases were not applied.

The global surveillance activities of the U.S. intelligence services revealed in 2013 by Edward Snowden also raise fundamental questions about data transfers between the EU and the U.S. based on the Safe Harbor agreement. With its trust in the U.S. handling of personal data permanently shaken, in summer 2013 the conference of federal and state data protection commissioners announced that they were checking whether data transfers by German businesses under the Safe Harbor system would have to be suspended. Reports by the Center for Digital Democracy, a U.S. consumer protection and privacy organization, of major violations of the Safe Harbor principles and lack of oversight by the Federal Trade Commission raised further doubts as to whether existing rules were being followed.

So the European Commission's intensive review of the Safe Harbor principles in late 2013 was both sensible and necessary. As well as the problem of U.S. intelligence services' access to data, the European Commission identified additional structural problems with the Safe Harbor principles, including problems of transparency, oversight and the enforcement of data subjects' rights; the review resulted in 13 recommendations for improving Safe Harbor. Contrary to the original plan, the talks between the European Commission and the U.S. authorities are still going on. The Conference of the data protection **commissioners of the Federal Government and of the States (Länder) therefore asked the Commission** president for a status report in late 2014.

More encouraging was the news that the FTC fined TRUSTe $200,000 in late 2014: TRUSTe, which many U.S. participants use to certify their compliance with Safe Harbor principles, had failed to conduct annual data protection inspections in more than a thousand cases from 2006 to 2013. Although the fine is rather low given the large number of cases and the length of time during which the failures occurred, I support every indication that the FTC is taking its data protection duties seriously.

The current discussion of Safe Harbor received a boost when the Irish high court presented a referral to the European Court of Justice dealing with the division of competences between the Commission and the Irish

data protection commissioner as well as with the impact of activities by the U.S. intelligence services on the reliability of the Safe Harbor principles. I am looking forward to the decision of the European Court of Justice, the political significance of which should not be underestimated.

4.7.2 BCR and CBPR proving difficult to reconcile

A comparison of EU and APEC requirements for approval or certification of rules on cross-border data transfers by private businesses shows some similarities, but mostly significant differences. The summary chart drafted by the Article 29 Working Party and the APEC's Data Privacy Subgroup is intended to help interested businesses prepare for the necessary examination procedures.

For the EU and the countries of the Asia-Pacific Economic Cooperation (APEC), special provisions apply to private-sector transfers of personal data to third countries. At EU level, these are binding corporate rules (BCR), which are anchored in Section 4c (2), first sentence, second half-sentence of Germany's Federal Data Protection Act; they are directed above all at multinational companies with multiple subsidiaries. At the level of APEC, the equivalent of BCR is the cross-border privacy rules (CBPR), which must comply with the APEC Privacy Framework adopted in 2005.

On the EU side, the approval procedures for BCR have proved effective over the years and have been considerably speeded up with the help of the mutual recognition process. In the meantime, dozens of BCR have been approved in Europe, including those of Deutsche Telekom AG in April 2014, under my supervision (see also No. 8.8.9).

By comparison, there is less experience with the CBPR system, which was only established in 2011, but a number of businesses in the U.S. have already been certified using this system.

Because many companies do business in both APEC and EU countries, they understandably asked for the approval procedures for BCR and certification for the APEC CBPR system to be combined into a kind of dual certification or at least simplified. To do so, a group made up of representatives from the Article 29 Working Party and the APEC Data Privacy Subgroup drafted a summary chart comparing the requirements for BCR approval and certification criteria for the CBPR system. On the EU side, the Article 29 Working Party adopted this document as its Opinion 2/2014 (WP 212 of 27 February 2014); on the APEC side, the document received support from the APEC Senior Officials Meeting 1 (SOM1) in February 2014. In early March 2014, the chart was presented to the public on the margins of the Global Privacy Summit of the International Association of Privacy Professionals (IAPP) in Washington, D.C. (see No. 3.1.3).

Although the chart was drafted with the aim of identifying what the two procedures had in common, it was soon clear that the differences far outnumbered the similarities, for example regarding the geographical scope of application, rights of data subjects and training requirements for staff involved in data processing in a business. Nonetheless, I hope the chart will help interested businesses in preparing BCR approval procedures or CBPR certification procedures.

The next task of the EU–APEC expert group is now to compile case studies for conducting the two procedures in practice, using examples of certified companies. This is intended to serve as the foundation for drawing up additional, practical information materials, such as checklists, for interested businesses.

I will continue to assist with the EU and APEC efforts to increase the interoperability of their data protection regimes and am participating in the current project of the joint EU–APEC data protection expert group.

4.7.3 New challenges regarding passenger name records

National legislation, demand by a wide variety of parties for the data and the problem of travelling jihadists have put law enforcement processing and use of passenger name records back on the political agenda. The European Parliament has asked the European Court of Justice to review the PNR agreement with Canada while opening the way for a European PNR system following the terrorist attacks in Paris.

Not too long ago, there seemed to be little news to report on this issue, a fixture of previous activity reports (see 22nd Activity Report, No. 13.5; 23rd Activity Report, No. 13.9; 24th Activity Report, No. 2.5.2) after the European Parliament held up the creation of a European passenger name record (PNR) system. PNR data were quietly transmitted to the U.S. and Australia on the basis of existing agreements. But then the debate over the purpose and usefulness of a European PNR system again picked up steam, for various reasons:

Firstly, various member states initiated national rules on creating PNR systems – ironically enough with funding from the European Commission, whose own proposal did not receive majority support in the European Parliament.

Secondly, already before the Ukraine crisis Russian had passed a law requiring airlines landing at Russian airports and flying over Russian territory to submit PNR data. It was possible to limit this initially to Advance Passenger Information (API), that is, data which can be retrieved from passengers' passports.

Due to the growing number of jihadists heading to Syria and Iraq, the political discussion of passenger name records had heated up already before the attacks in Paris. The argument that passenger name records could significantly help fight terrorism gave new impetus to the debate at European level. After the Paris attacks, the issue of PNR was central to the measures discussed in reaction to the attacks. The European Parliament has reacted to this. By the majority, it gave up its fundamental opposition, thereby making it possible to create a European PNR system.

I continue to doubt whether storing the passenger name records of all airline passengers in the absence of concrete suspicions is necessary or proportionate. At the time this report went to press, no new legislative proposal had been drafted. Whether storing such data is lawful will largely depend on what restrictions on the processing of passenger name records result from the European Court of Justice judgment on the retention of telecommunications data (see No. 2.3.1). I believe that this judgment is very relevant for the retention of passenger name records as well, and the majority of the European Parliament seems to share this view, as the Parliament has asked the Court to review the PNR agreement between the EU and Canada. Clearly, the European Court of Justice is increasingly taking on the role in the field of internal security played by Germany's Federal Constitutional court in the years after 9/11: setting the boundaries of lawfulness in counter-terrorism and occasionally having to restrain lawmakers in the process.

7.3 SWIFT agreement

The first request for information under the SWIFT agreement was sent to the U.S. Treasury.

The SWIFT agreement concluded between the EU and the U.S. in 2010 is supposed to detect the movement of payments intended for terrorist financing; it provides a right of access for data subjects (Article 15) as well as a right to rectification, erasure or blocking (Article 16) of data sent to the U.S. under the terms of this agreement. Although these are personal rights of data subjects, they can only be claimed by going through the national data protection authority, which then sends the request for information, rectification, erasure or blocking to the U.S. Department of the Treasury (DoT).

In 2013, the EU and the DoT agreed to simplify this complicated procedure by having the national data protection authority verify the requester's identity. Copies of official identity cards do not have to be sent to

the U.S., as originally agreed. After verifying the identity of the person making the request, the national data protection authority forwards the request to the DoT. The DoT does not respond directly to the requester; its response is also sent via the national data protection authority.

Experience has shown that EU citizens are not sufficiently familiar with their right of access. Although the agreement was adopted in 2010, Germany was the first EU member state to submit such a request to the DoT, in November 2013. With a reference to Article 15 (2) of the agreement, the response was very brief, but it did confirm that the requester's data protection rights had not been violated.

I will continue to monitor the implementation of the agreement and help individuals with their requests for information about their personal data (see 23rd Activity Report, No. 13.6 and 24th Activity Report, No. 2.5.1).

7.5 Foreign Account Tax Compliance Act (FATCA)

In 2014, data on persons subject to U.S. taxes were collected under the FATCA agreement for the first time.

The bilateral FATCA agreement between Germany and the U.S. entered into force on 11 December 2013. It clarifies the framework for the U.S. and German tax authorities to regularly share information on private bank accounts in order to ensure effective taxation. The agreement was needed after the U.S. passed the Foreign Account Tax Compliance Act (FATCA) in March 2010 covering assets held outside the U.S. by persons and organizations subject to U.S. taxes. Enforcing the Act led to major conflicts with data protection law in Germany and Europe (see 24th Activity Report, No. 2.5.5).

I was involved from the start at both European and national level in the process of implementing FATCA and worked to ensure a reasonable level of data protection, in particular by insisting on the data protection principles of necessity and purpose limitation.

The FATCA Agreement to Improve International Tax Compliance is now being implemented via Section 117c of the German Fiscal Code (*Abgabenordnung*, AO). I advised making use of the authorization in Section 117c AO to issue statutory instruments in order to govern details of form, content, processing and security of data to be transferred to Germany's Federal Central Tax Office (BZSt).

The ordinance implementing the obligations arising from the FATCA Agreement (*FATCA-USA-Umsetzungsverordnung*) and governing the collection and transmission of the necessary data by financial institutions entered into force on 29 July 2014. German financial institutions reporting data are required to register with the U.S. Internal Revenue Service (IRS) and to report the required data on financial accounts to Germany's Federal Central Tax Office. The data are to be collected annually starting in 2014 and reported to the Federal Central Tax Office by 31 July of the following year, which will forward this information to the IRS.

The Federal Central Tax Office will also forward to the responsible tax offices in Germany information provided by the IRS on persons who have bank accounts in the U.S. and are subject to German taxes.

I will continue to monitor this procedure for compliance with data protection law (see 24th Activity Report, No. 2.5.5).

7.10 Fourth anti-money-laundering directive

A new EU directive is intended to improve the fight against money laundering and terrorist financing.

International legislation plays a key role in fighting money laundering. The last three anti-money-laundering directives, which primarily targeted drug crime and terrorism, have been transposed into national law relating to money laundering. Since 2012, a fourth directive on money laundering has been in preparation (Directive of the European Parliament and the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing). This directive is intended to create a consistent regulatory framework to fight money laundering and terrorist financing while taking into account revised international standards presented in February 2012 by the Financial Action Task Force (FATF) working group on measures to fight money laundering.

The new rules will allow a more efficient response to new threats from money laundering and terrorist financing. The new directive will have an expanded scope and stricter due diligence obligations and will improve the identification of the individuals behind a business.

The European Commission adopted the first proposed revision of the new directive already in February 2012; in March 2014, the European Parliament agreed on a preliminary legislative outline containing some improvements relating to data protection law and a demand to introduce a central register for identifying beneficial owners. After publishing a general approach on the 4th anti-money laundering directive in June 2014 that differed from the parliamentary proposal, the Council was able to agree with the Parliament on a common proposal. The compromise text now requires only formal approval from the plenary of the European Parliament and the Council.

The Commission consulted the European Data Protection Supervisor (EDPS) at a late stage in the process, and then only informally. The draft directive was not presented to the Financial Matters Subgroup of the Article 29 Working Party, and thus also to the data protection commissioners, until February 2013 (see No. 3.1).

The Article 29 Working Party wrote two letters, in April and November 2013, to the European Parliament expressing its data protection concerns. The scope of the anti-money-laundering directive is supposed to extend well beyond the original goals of fighting money-laundering and terrorism to include tax crime as well. But the terms are not sufficiently defined, nor does the draft clearly define the intended purpose and the purpose limitation. I also fear that, as planned, the simplified due diligence obligations no longer conform to the risk-based approach pursued up to now, meaning that data could be collected arbitrarily and in excessive amounts. The Article 29 Working Party therefore calls for special regulations for the transfer of personal data to third countries lacking a sufficient level of data protection.

The EDPS is also critical of the Commission’s proposal and, in his opinion of February 2014, recommended improvements to data protection. He called for applying EU data protection law, paying greater attention to purpose limitation and providing data subjects with the right to know about the processing of their data.

I will continue to follow the process in a spirit of constructive criticism, at European level through my participation in the Article 29 Working Party and with regard to its implementation at national level.

8.7 TTIP

The negotiations on the Transatlantic Trade and Investment Partnership (TTIP) are proceeding without the involvement of the data protection authorities. The negotiations must not be allowed to weaken European standards of data protection.

The current, largely secret, negotiations between the European Commission and the U.S. on TTIP give reason for data protection concerns due to the intended aims of the agreement, in view of the economic interests of international companies, to reduce barriers to trade. After all, the central reason for the EU’s Data Protection Directive (95/46/EC) was to reduce non-tariff barriers to trade.

In its resolution on ensuring data protection in a transatlantic free-trade zone, the 85th conference of the data protection commissioners of the Federal Government and of the States (Länder) (13 March 2013; see Annex 5) called on the European Commission to remain focused in the negotiations on the goal of a community of values based on fundamental rights and to uphold the fundamental right to data protection guaranteed by the EU Charter of Fundamental Rights and the standards based on them.

I would like to be able to see the planned TTIP provisions for myself and form an opinion of their impact on data protection, but like all other data protection authorities, I am not allowed to take part in the negotiations. I find it all the more unfortunate that I am not allowed to participate in the Federal Ministry of Economics and Technology's TTIP advisory council convened in May 2014, although data protection issues play at least an indirect role there. Nor has the Federal Government responded to my requests for at least rudimentary information on data protection issues in TTIP.

The negotiating mandate issued by the European Council to the European Commission does not mention data protection. By contrast, the free trade agreement already negotiated with Canada (CETA) explicitly exempts data protection. Since CETA is regarded as a model for TTIP, I hope the latter will adopt this arrangement too.

I am pleased that the Federal Government responded to a minor interpellation in the German Bundestag by stressing that it in principle always represented the position that the free trade agreement must not lead to lower standards of data protection and must be ratified not only by the EU but also by the member states (Bundestag printed document 18/2687, pp. 2 and 5).

I am happy to advise the Bundestag on data protection law issues ahead of this ground-breaking decision.

14.6 eCall: Using personal data to save lives

The eCall system has the potential to save many lives by alerting emergency responders more quickly, but it also entails privacy risks which European law in principle takes into appropriate account.

Following an amendment of EU type-approval rules, all new models of cars will have to have built-in eCall systems starting in 2018: In case of a serious car accident, a predefined set of data will be sent automatically or manually by a vehicle occupant to the nearest emergency call centre, immediately triggering an emergency response. Voice communications to the vehicle can also be established.

Data sent include the physical location of the vehicle and its direction of travel, the time and the vehicle identification number. But such automatic data transfer which as a rule is independent of the data subject's control also entails privacy risks. I am involved in the legislative process at EU level through the Federal Ministry of Transport and Digital Infrastructure (BMVI). I have also participated in the meetings of the national eCall implementation platform.

Provisions on eCall can be found in a decision requiring member states to create a network of emergency call centres to process incoming eCalls. Data sent to the call centres may only be used for the emergency response purposes pursued by the decision. In Germany, the federal states are responsible for building and operating these call centres in a manner consistent with data protection.

In addition to this decision, an EU regulation will govern the specifications for the technology to be built into cars. At the time this report went to press, the negotiations on this regulation had not been completed, so I have not yet seen the definitive text, but it probably contains relatively detailed data protection rules. The main thing is that the eCall system should not be able to track vehicles during normal operations, that is, in the absence of a serious accident which would set off an eCall. Unfortunately, it was impossible to give vehicle owners or users the possibility to deactivate the built-in eCall system.

At the time this report went to press, it was not yet clear how eCall, which will be included in every vehicle, will work with manufacturers' own emergency call services; eCall and such manufacturer-specific systems will probably not both be active at the same time. eCall is however supposed to go into operation if the vehicle owner has not subscribed to the optional service, or if it fails to function. Ultimately, however, regardless of the technology, such services should be clearly distinguishable from the eCall service, so that drivers may decide whether to use the manufacturer's service, which may transmit more data from the vehicle than necessary, instead of the eCall service.