Extracts from the 2017/2018 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information – 27th Activity Report

1 Main topics – national level

1.1 Implementation of the General Data Protection Regulation (GDPR)

My activities in the years 2017 and 2018 were essentially driven by the implementation of the General Data Protection Regulation which, when it came into effect on 25 May 2018, placed European and German data protection law on a completely new legal footing, thereby initiating a new era of data protection. This posed enormous challenges for my organisation.

Introduction

In addition to monitoring the federal legislator's relevant adaptation legislation, interpretation aids for practical application had to be developed or existing documents revised both at national level by the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder (DSK, *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*) and at European level by the Article 29 Working Party and the European Data Protection Board (EDPB, see No. 2.1). The EDPC, for instance, has produced almost twenty so-called short papers on certain issues of the GDPR in which the German supervisory authorities present coordinated, uniform views on various core issues of the GDPR (available at: www.datenschutz.bund.de, see also No. 17.9). Both in the Article 29 Working Party and, after 25 May 2018, in the EDPC, my authority had a major role to play in the development of various guidelines for the GDPR, for instance, on priority topics, such as consent or accreditation of certification bodies specifically for data protection issues.

My press and public relations team also had to cope with a substantial workload. These tasks included revising almost the entire information material which I post as brochures, flyers or articles on my website (see No. 17.9 below). Inquiries and complaints from citizens as well as the number of reported data protection violations have also risen sharply since 25 May 2018 (see above: BfDI's work in figures). This shows that there is an enormous need for advice and information among controllers and citizens alike.

After all, my authority in its capacity as a supervisory authority also had to implement the GDPR, which called for organisational and substantive innovation (see No. 17.1 below). Since my agency itself also processes personal data, I had to implement the GDPR in my role as a controller within the meaning of data protection legislation.

Adaptation legislation

The German legislator made the adaptation of national data protection law to the GDPR and the implementation of the Directive on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences (JHA Directive, see also No. 1.2 below) the subject of two major legislative procedures.

The Federal Data Protection Act (BDSG, *Bundesdatenschutzgesetz*), in particular, was revised with the Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Di-

rective (EU) 2016/680 (EU Data Protection Adaptation and Implementation Act (DSAnpUG-EU, *Datenschutz-Anpassungs- und Umsetzungsgesetz EU*). Since 25 May 2018, this has supplemented the directly applicable GDPR in areas where the GDPR leaves the Member States room for their own preferences or issues regulatory mandates. Furthermore, the Federal Data Protection Act implements essential parts of the above-mentioned Directive 2016/680. The new Federal Data Protection Act applies – just like the Federal Data Protection Act (old) – to public bodies of the Federation as well as to non-public bodies. It only applies to public bodies of the federal states (*'Länder'*) in as far as there are no regulations under federal state law. In order to facilitate as uniform a development as possible of general data protection law, the Federal Data Protection Act also applies to personal data processing activities by public authorities of the Federation that do not fall within the scope of European law (for instance, intelligence services, Bundeswehr).

My initiative made it possible to achieve some improvements in legislation compared to the preliminary drafts, including the central principle of earmarking in the public sector. I am still sceptical about other provisions of the new Federal Data Protection Act, for instance, the limited powers of supervisory authorities in relation to holders of confidential information, such as lawyers, pursuant to sec. 29 BDSG. The same applies to my limited supervisory powers in the police and judiciary sectors and outside the scope of European law. Independent control is absolutely necessary, especially for secret data collection. However, instead of improving citizens' confidence in data collection operations by government in this area, I do not have any effective enforcement powers here; the only instrument available to me are non-binding complaints. I consider this to be a violation of the constitutional and European principles of strong and independent data protection supervision (see No. 1.2 et seq.). Fundamental adaptations to the GDPR as of 25 May 2018 were also made in social and tax procedural law (see No. 3.1.1, No. 6.1.1).

The 'Second Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680' (2. DSAnpUG-EU, *Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU*) is now also to adapt larger parts of the remaining sector-specific federal data protection law to the GDPR. The draft law introduced by the Federal Government (Bundestag document (*BT-Drs.*) 19/4674) provides for changes in 154 sectoral laws of almost all departments. The main areas of regulation include the adaptation of definitions and legal principles for data processing as well as regulations regarding the rights of data subjects. In my statement, I pointed out the need for improvement, including the planned amendments to the Act on the Establishment of a Federal Institute for Digital Radio of Authorities and Organisations with Security Responsibilities (BDBOS-Gesetz, *Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben*). I also demanded that corresponding wording in the Fifth Book of the Social Code (SGB V, *Fünftes Buch Sozialgesetzbuch*) stipulate that fines may also be imposed on statutory health insurance funds in the event of violations of the GDPR. I do not see any reason why the statutory health insurance funds, which increasingly see themselves as commercial enterprises with an expenditure volume sometimes exceeding 25 billion euros, should be given privileged treatment compared to crafts or small industrial companies. I take a particularly critical view of the fact that this act also fails to address the mandatory amendments to the Telecommunications Act (TKG, *Telekommunikationsgesetz*). This complicates the application and enforcement of data protection law in the telecommunications sector and leads to considerable legal uncertainty (see point 15.1.1).

On 12 October 2018, the Bundestag referred the draft of the Federal Government to the Committee on Internal Affairs after the first reading of the bill. The parliamentary procedure is to be continued at the beginning of 2019.

Implementation at companies and authorities

Unfortunately, many stakeholders failed to make sufficient use of the two-year transitional period before the GDPR came into effect in order to adequately prepare themselves for the new rules. These shortcomings are illustrated by a representative survey of 505 companies which was conducted by the Bitkom industry association shortly before the end of the two-year transitional period on 25 May 2018. Only a quarter (24 percent) of the companies surveyed in Germany stated that they had almost fully implemented the new regulations by the end of the deadline. Another third stated that they were able to achieve this goal at least in part. Four percent of the companies were only at the beginning of their efforts and two percent of the companies surveyed had to admit that they would not be able to take even first steps towards implementation by the time the deadline expired. However, four months after the deadline, the world looked a little better.

According to another representative survey, many of the 502 companies surveyed are still struggling with implementation after the deadline. The extended documentation and information obligations were one of the aspects they criticised. Just a quarter (24 percent) of the companies in Germany had fully implemented the GDPR. That being said, however, another 40 percent had implemented most of the rules and 30 percent at least part of them. Only five percent of the companies had just begun making adjustments. Overall, it can be seen that efforts by the supervisory authorities are still necessary in order to raise awareness among companies regarding the requirements of the GDPR. As far as the implementation of the GDPR at the federal authorities under my control is concerned, it can be said that, even though there was considerable demand for information and advice, the new regulations were by and large consistently implemented. I supported this process with my brochure 'Die DSGVO in der Bundesverwaltung' (*The GDPR at the Federal Administration*) (available at www.datenschutz.bund.de).

Impact of the GDPR in everyday life

It comes as no surprise that a completely new law in such an important cross-cutting area as data protection cannot be introduced completely without friction or debate. Unfortunately, media coverage of the GDPR and the related debate did not always focus on the advantages and opportunities of a harmonised European data protection law, but – understandably – on certain questions regarding its specific implementation. This led to a great deal of uncertainty. It was frequently found that misinformation was disseminated or that regulations, which had existed under the old law for decades, were referred to with reference to the new GDPR (see also the information box regarding No. 1.1). This has damaged the general public's acceptance of the new legislation. Many reports concerned presumed or real everyday stories, such as photographs in kindergartens, the fitting of bell signs or the widespread fear of cease and desist requests:

→ Dealing with photographs

In the summer of 2018, I received numerous enquiries from citizens after a series of press articles had stirred up considerable uncertainty. Even in the early days after the GDPR came into effect, a broad public debate had started regarding the handling of photographs in compliance with data protection regulations, be it in sports, at kindergartens or by journalists. However, the GDPR did not change anything material in this respect compared with the legal requirements already in place. The following is still valid: If imagery is created by natural persons within the scope of exclusively family or private activities, data protection law does not apply from the outset. This is, for example, always the case when a family member takes photographs or videos at a private family celebration and does not publish such material. In as far as data protection law does apply, it is still possible to take and process photographs if the interests of all parties have been carefully weighed. The following rule of thumb applies to cases like these: The smaller the encroachment upon personality rights (for example, in the case of overview photo-

graphs, photographs in stadiums or at public events, etc.), the more likely it is that this weighing of interests will be in the photographer's favour. This can also apply to persons in special need of protection, such as children, in as far as not only the photographer's interests are pursued, but also, for example, those of the child itself and other children at the same time – as in the case of photo albums given as gifts to children leaving kindergarten. None of this is new, and everything is largely identical to the pre-existing legal situation. In contrast, consent is still only necessary in a few cases, especially if the interests of the data subject not to be photographed prevail. Consent may therefore be necessary, for instance, in the case of portrait photographs or if a photograph shows a situation that is not socially adequate. The publication of pictures on the Internet continues to be subject to the Art Copyrights Act (KunstUrhG, *Kunsturhebergesetz*) which protects the right to one's own picture, an issue that has meanwhile been confirmed by the courts. This law allows pictures of gatherings or parades, such as folk festivals, processions, etc. to be published without consent. This legal situation has applied for decades and has not been changed by the GDPR.

→ Bell signs

A particularly bizarre example was the question as to whether or not bell signs with names will be banned on apartment buildings in the future. In this respect, I – like many of my colleagues in the federal Länder – made it clear that data protection law is definitely not applicable since the GDPR applies only to automated data processing or processing in file systems.

→ Cease and desist requests

Before the GDPR came into effect, there was much talk about waves of cease and desist requests that would hit small and medium-sized enterprises or associations that hardest. This predicted wave of cease and desist requests has resulted in fewer than five complaints regarding such actions still pending in my authority at the end of 2018.

Special application cases of the GDPR

When implementing and applying the GDPR in Germany, existing constitutional requirements must be taken into account. In the field of legislative work by the German Bundestag, for example, I may only act in an advisory capacity (see No. 14.1.1 below).

The provisions of the GDPR only apply to a limited extent to the processing of personal data by broadcasting and media companies. This follows from the constitutionally guaranteed freedom of press and radio reporting (Art. 5 (1) of the Basic Law for the Federal Republic of Germany (GG, *Grundgesetz für die Bundesrepublik Deutschland*), a relevant regulatory mandate under Art. 85 GDPR and the relevant provisions in the State Broadcasting Treaty (RStV, *Rundfunkstaatsvertrag*) where data protection regulations are replaced primarily by data protection regulations specific to broadcasting operations (sec. 9c and sec. 57 of the State Broadcasting Treaty). Art. 91(1) GDPR contains a grandfathering provision for churches or religious associations. This means that, should churches or religious associations apply their own comprehensive data protection regulations when the GDPR comes into effect, they can continue to apply these regulations if they are harmonised with the GDPR. If, in contrast, churches and religious associations do not have a comprehensive set of data protection regulations when the GDPR comes into effect, the GDPR will apply in conjunction with the Federal Data Protection Act.

Independent supervisory authorities can be established for the areas of broadcasting and media as well as churches and religious communities (art. 85 (2), art. 91 (2) GDPR). German media companies, broadcasting corporations as well as the Catholic dioceses and the Evangelical Church in Germany (EKD, *Evangelische Kiche in Deutschlad*) have each appointed their own data protection officers or set up their own data protection authorities (regarding Deutsche Welle, see No. 10.1.1 below). Since each Member State, regardless of the number of data protection authorities set up, can speak with only one voice in the European Data Protection Board (EDPD), the

German supervisory authorities must first coordinate their activities (see No. 17.3 below). In these coordination measures, the general data protection supervisory authorities of the Federation and the Länder are obliged to also involve the specific supervisory authorities set up in accordance with art. 85 and 91 GDPR in as far as this concerns them (sec. 18 (1) 4th sentence of the Federal Data Protection Act). My authority has hosted several constructive rounds of talks with representatives of the data protection authorities of churches, religious communities, media and broadcasting, in which the Presidency of the Data Protection Conference was also involved.

I recommend that the legislator make it clear that fines can also be imposed on statutory health insurance funds for violations of the GDPR if they act as commercial enterprises.

A particularly bizarre reference to data protection under the GDPR occurred in Berlin where a customer complained about a butcher's shop assistant addressing her by name. The customer claimed that using her name to address her was not permitted under the GDPR (Berliner Morgenpost, online edition of 11 Dec. 2018). Such a rejection of a friendly greeting is as bewildering as the reference to data protection in this regard. The GDPR deals exclusively with fully or partially automated processing of personal data and the non-automated storage of personal data in a file system. A sales assistant's ability to remember names, however, is certainly not a file system within the meaning of the GDPR.

1.2 Transposition of Directive (EU) 2016/680

Since 6 May 2018, uniform minimum standards for data processing by police and judicial authorities must be implemented in all Member States.

In my last activity report, I reported on the obligation to implement the minimum requirements of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (see 26th Activity Report, No. 1.2.2). In the meantime, the transposition deadline has expired and the federal legislator has generally transposed the requirements of the Directive into national law with the new Federal Data Protection Act. The essential part of these regulations is summarised in the third part of the Act, and the first part of the Act contains certain regulations that are commonly applicable to all areas.

Several sectoral laws also had to and still have to be successively adapted. The new Federal Criminal Police Act (BKAG, *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*) marks the beginning of this effort (see below No. 9.1.3). Draft laws for the implementation of the JHA Directive exist for the Customs Investigation Act (ZfDG, *Gesetz über das Zollkriminalamt und die Zollfahndungsämter*) and the Code of Criminal Procedure (StPO, *Strafprozessordnung*) (see No. 9.1.4 and No. 11.1.2 below). A draft amendment to the Federal Police Act (BPolG, *Gesetz über die Bundespolizei*) is still pending. The specific features of the Directive include obligations to keep records as well as requirements regarding the design of databases, the special supervisory function of supervisory authorities in conjunction with the restriction of the rights of data subjects (so-called indirect access) and the powers of supervisory authorities, which are regulated only in terms of their nature.

The federal legislator did not follow my recommendation to regulate the powers of supervisory authorities in analogy to the GDPR (see 26th Activity Report, No. 1.2.2). Although I have extensive powers of information and investigation, the only remedy that remains, as before, is complaint. The new Federal Criminal Police Act at least provides for the

authority to issue orders in response to complaints about significant data protection violations. The new draft Customs Investigation Act also contains a corresponding proposal, and I expect that a corresponding regulation will also have to be created in the Federal Police Act. This is because the complaint instrument alone is not sufficient to meet the requirements of the Directive, which require the supervisory authorities to be able to remedy the situation effectively. I consider the lack of harmonisation in the transposition of the Directive to be a generally unfavourable development. The scope of application is linked to the concept of a criminal offence, which is not conclusively defined in the Directive. This provides scope for implementation, especially when it comes to prosecuting and defending against administrative offences. This scope is addressed differently both within Germany and at EU level. This ranges from the full inclusion of the prosecution of administrative offences (for instance, at federal level in Germany) to the restriction to formal offences under national law (such as in several other Member States). Due to the vague specification, it was unfortunately not possible to achieve even a minimum degree of harmonisation in this area.

The next few years will show how the new regulations will succeed in real life. Many individual questions are still open, such as the design of the mandatory public directory of procedures, the performance of data protection impact assessments, the reporting and information obligations in the event of data protection violations or the scope of logging.

I recommend that the legislator include remedial powers for the Federal Commissioner for Data Protection and Freedom of Information in the new Federal Police Act. These powers should at the very least correspond to the powers already contained in the new Federal Criminal Police Act.

1.2.1 'GDPR-free spaces' in the area of intelligence services

The provisions of the GDPR do not affect the work of the Federal Intelligence Service (BND, *Bundesnachrichtendienst*) or the performance of tasks by the Domestic Intelligence Service (BfV, *Bundesamt für Verfassungsschutz*) or the Military Counter Intelligence Agency (MAD, *Militärischer Abschirmdienst*). However, certain basic rules apply to military intelligence.

The effects of the GDPR and of the Directive on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences (JHA Directive) are relatively limited in the area of intelligence services and security clearance law. Neither the GDPR nor the JHA Directive are applicable to the law of intelligence services in the narrower sense or the Security Clearance Act (SÜG, *Sicherheitsüberprüfungsgesetz*). The intelligence services are only obliged to apply the GDPR in the general administration of public agencies. Although the national legislator has declared individual terms and certain standards, which it issued in addition to the GDPR and/or in transposition of the JHA Directive, to be (analogously) applicable to the intelligence functions of the Federal Intelligence Service, the Domestic Intelligence Service and the Military Counter Intelligence Agency as well as in the Security Clearance Act, everything essentially remains as it was before in this area.

The Military Intelligence System (MilNw, *Militärisches Nachrichtenwesen*) is an exception: As its name already suggests, this area of the Bundeswehr is, similar to intelligence services, designed for intelligence and information gathering, which can also affect the collection and processing of personal data. In individual cases, the means used for this purpose are similar to those known from the intelligence sector. This is why I have always argued that special legislation is required as a basis for this area too. This is still lacking. The Federal Ministry of Defence (BMVg, *Bundesministerium der Verteidigung*) takes a different view. It considers art. 87a and art. 24 (2) of the Basic Law to be a sufficient constitutional basis for action by the Bundeswehr

within the framework of the Military Intelligence System and for the processing of personal data in this context. Notwithstanding this, the Federal Ministry of Defence is currently working on a decree on how the requirements of the Federal Data Protection Act can be implemented for the Military Intelligence System. This also concerns the rules for reporting data protection violations and the obligation to perform a data protection impact assessment. I am currently in talks with the Federal Ministry of Defence on this topic. During the course of the implementation of the GDPR and the JHA Directive, the legislator also amended the Federal Intelligence Service Act, (BNDG, *Gesetz über den Bundesnachrichtendienst*) the Federal Constitutional Protection Act (BVerfSchG, *Bundesverfassungsschutzgesetz*) and the Military Counter Intelligence Agency Act (MADG, *Gesetz über den militärischen Abschirmdienst*). In contrast to the scope of the GDPR and the JHA Directive, I still have no powers to impose sanctions on intelligence services if I consider the processing of personal data to be unlawful. Cessation of unlawful activities by intelligence services can therefore still today only be enforced by legal action by data subjects, which is in fact very difficult to achieve given the limited scope of legal protection available to the data subjects concerned.

I therefore recommend that the legislator introduce sanction powers for my authority which also apply to intelligence services.

1.3 New developments in the field of border control and passenger data

Security authorities are increasingly focusing on travel data. Over the coming years, the existing information systems will be fed with ever-more data, new systems will be added and all systems will be interconnected under the umbrella of interoperability according to a draft regulation that is currently being negotiated. The aim is to curb identity fraud and the associated security risks. This project will create enormous challenges for data protection supervisory authorities.

In my past Activity Reports I critically examined both the projects pursued under the 'Smart Borders' keyword (see 24th Activity Report No. 2.5.3.4; 25th Activity Report No. 3.3; 26th Activity Report No. 2.3.1) as well as all projects relating to the use of passenger data for security purposes (see 22nd Activity Report No. 13.5.5; 26th Activity Report No. 2.3.2). In the meantime, a new stage has been reached in all these areas. The first new large database was launched at the end of December 2017 with Regulation (EU) 2017/2226 establishing an Entry Exit System (EES). On this basis, a database will be set up in which all border crossings by third-country nationals at the external Schengen borders will be recorded and stored for at least three years from the date of departure. The data set includes photographs and fingerprints. If less than three years have lapsed between departure and next entry, all existing data will also continue to be stored. This automatic drag-along mechanism can produce comprehensive travel histories. The second new database will complement the Visa Information System (VIS). The legal basis for the new European Travel Information and Authorisation System (ETIAS) came into effect with Regulation (EU) 2018/1240 at the end of October 2018. All third-country nationals entering under a visa waiver programme will be required to apply for an entry permit in advance. Their data is subjected to an early automated check for security, migration and health risks and is typically stored for three years or, if rejected, even for five years.

The development of new databases will be accompanied by extensive upgrading and expansion of existing databases. In future, VIS will also cover long-term visas and residence permits (see No. 2.2). The Eurodac asylum system will also register third-country nationals who are found during an illegal stay or illegally crossing a border. The second-generation Schengen Information System (SIS II) will be supplemented by new alerts (for instance, for covert investigation/questioning) and data categories (such

as handprints) and will be made available for repatriation management of illegal third-country nationals. The new regulations were already adopted by the copy deadline, but had not yet been signed and announced.

Two other proposals for regulations on so-called interoperability are currently under discussion and will link the above databases using a common search mask (European Search Portal, ESP) and three new databases in order to detect and prevent identity fraud. All existing biometric identification data will be converted to so-called templates (mathematical maps) and stored in a shared Biometric Matching Service (sBMS) for fast database matching. The specialist applications, i.e. VIS, Eurodac, EES and ETIAS, will also be provided with a common identity repository (CIR) in which all identity data, including biometric originals, will be stored. Only the SIS data will remain outside the CIR for technical reasons. Each time data is entered or updated in the specialist applications, the first step will then be to match this data with the sBMS and the ESP (in the SIS and in the CIR). Hits will be reported to the responsible authorities for processing and simultaneously stored in the Multiple Identity Detector (MID) according to several categories.

Although both the data protection authorities of the Member States and the European Data Protection Supervisor have taken a critical view and have voiced various concerns with regard to all legislative acts, they received little attention. The targeted extension of existing information systems, along with the development of new databases and the proposed complex interoperability system, are extremely worrying. In particular, the principle of limiting the purpose for which data is collected is at risk of being increasingly eroded. The identification of third-country nationals by means of a comprehensive biometric and alphanumeric identity register becomes a multidisciplinary end in itself.

The data available is further condensed by the Passenger Data Directive that has since been implemented in various countries. In Germany, the Passenger Data Act (FlugDaG, *Fluggastdatengesetz*) has been in effect since June 2017, obliging all air carriers to transmit the passenger data (so-called Passenger Name Records, PNR) collected by them for the purpose of providing a flight service (except for domestic flights) to a Passenger Information Unit (PIU) set up for this purpose at the Federal Criminal Police Office (BKA, *Bundeskriminalamt*). Comparable measures must be taken in all Member States. In Germany, the PIU went live at the end of August 2018. Incoming passenger data may be matched with both search databases and abstract threat patterns. As a result of such matching, passengers may be targeted by police measures without themselves having given any concrete reason for this, simply because there are similarities to the behaviour of offenders. This alone is already highly questionable.

In addition, there is the five-year retention period for all passenger data which enables retroactive searches to be carried out in order to prevent and prosecute terrorist or other serious crimes. In this case, a long-term database is created at a police authority about persons who, for the most part, have not given cause for their entry in a precautionary policy database other than travelling by air. I also consider this to be extremely questionable, especially since the European Court of Justice has now, in an opinion on the proposed EU-Canada passenger name records agreement, criticised long-term storage without cause as being incompatible with the Charter of Fundamental Rights of the European Union.

I recommend that the Federal Government revise the Passenger Data Act with regard to the requirements of the European Court of Justice regarding the passenger name records agreement with Canada and advocate a revision of Directive (EU) 2016/681 in Brussels.

Data Ethics Commission – DEC

The DEC was established by the Federal Government in autumn 2018. The task of the DEC is to develop recommendations for action for the Federal Republic of Germany's future data policy by autumn 2019. The DEC is tasked with the development of guidelines for the protection of the individual, the maintenance of social coexistence and the safeguarding and promotion of prosperity in the information age. Furthermore, recommendations for action should be made as to how these ethical guidelines can be developed, observed, implemented and supervised. The DEC has 15 other members besides me. The members are representatives of data protection supervisory authorities, professors from various disciplines as well as representatives of consumer protection organisations and industry. Further information is available from the DEC website at https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html

1.4 Artificial Intelligence

On 15 November 2018, the Federal Cabinet adopted the Artificial Intelligence (AI) Strategy jointly presented by the Federal Ministries for Economic Affairs and Energy, of Education and Research as well as of Labour and Social Affairs. With the Artificial Intelligence Strategy, the Federal Government aims to develop Germany and Europe as a leading centre for innovation and the application of AI technologies, thereby securing Germany's competitiveness.

The bandwidth and application possibilities of AI are already enormous today. They range from the simple calculation of itineraries to image and speech recognition as well as extremely complex decision and prediction environments. Self-learning algorithms continuously monitor and update their own calculation processes. One foreseeable trend is the development of ever-more independent and comprehensive applications which will automate and in part replace more and more human behaviour in ever-broader fields of action. The amount of personal data that is processed will increase. At the same time, the processing paths are becoming increasingly difficult for data subjects to understand. The risks associated with AI technologies for the informational self-determination of individual data subjects are therefore just as complex as their possible applications. I therefore accompanied the development of the AI strategy and I have worked to ensure that the protection of privacy is understood to be an essential part of the promotion of innovation and that the requirements of the GDPR be seen from the very beginning to be quality characteristics for the responsible development and use of AI in the interest of the common good. At the beginning of September 2018, we discussed the Federal Government's key issues paper and drew up data protection recommendations for the AI strategy in the Data Ethics Commission (DEC – see information box).

With this as a basis, I was able to introduce important data protection aspects at the 'World of Work and Labour Market' (*Arbeitswelt und Arbeitsmarkt*) forum held by the Federal Ministry of Labour and Social Affairs in mid-September 2018, the results of which were then incorporated into the AI strategy. Important issues, such as employee data protection in the area of AI applications, the use of advanced pseudonymisation and anonymisation methods, the need for technology assessments or the development of large amounts of data in compliance with data protection regulations, have been taken into account at several points within the AI strategy. The recommendations by the DEC are referred to several times. Furthermore, the establishment of a round table with representatives of data protection supervisory authorities and business associations is announced in order to develop both common guidelines for the development and application of AI systems in compliance with data protection law and best-practice application examples. All in all, I am pleased to report that the perspective of data protection is

mentioned at many points in the AI strategy. It remains to be seen whether and to what extent this perspective will then also be taken into account in the further implementation of the strategy. I will critically accompany the further elaboration and implementation of the AI strategy.

The Conference on Data Protection, the body of independent German federal and Länder data protection supervisory authorities, will also address data protection issues in the use of artificial intelligence in 2019.

In October 2018, the International Conference of Data Protection and Privacy Commissioners adopted a statement regarding ethics and data protection for AI. This resolution sets forth, for instance, six principles that should always be observed in the application of artificial intelligence:

→ Fairness

→ Traceability

→ Transparency

→ Privacy by design

→ Strong rights of data subjects

→ Avoidance of built-in prejudices or discrimination

I strongly support this resolution and believe that it can serve and help the international data protection community to develop certain guiding principles for the development and use of systems incorporating artificial intelligence. This applies, for instance, to applications of artificial intelligence in handwriting, image and facial recognition, autonomous motor vehicles, search engines, diagnostics and marketing, as well as further development possibilities.

1.4.1 Blockchain – without data protection?

The German government plans to present a blockchain strategy by mid-2019. The Federal Ministry for Economic Affairs and Energy and the Federal Ministry of Finance are the leading bodies for this strategy. A consultation process has been designed to ensure that indications and recommendations from market players, academia and other stakeholders regarding the need for policy action are taken into account. Blockchain generally means a continuously expandable list of data records – called blocks – which are linked together by cryptographic methods. Each block contains the hash value of the previous block, a time stamp and transaction data. This means that the existence and content of individual blocks cannot be changed later without this leading to irregularities in all of them. The great advantage of the blockchain is the fact that the data chain cannot be compromised, so that it is suitable for financial transactions. In this respect, the term 'blockchain' is associated with distributed ledger technology. The 'distributed ledger concept' refers to a public, decentralised account book and is the technological basis of virtual currencies.

The German government supports blockchain pilot projects in the areas of electric mobility, electricity trading and migration. I have examined the possible use of blockchain technology at the Federal Office for Migration and Refugees specifically with regard to design and implementation in compliance with data protection legislation (see No. 9.3.1 below). The central challenges in the use of blockchain technology in compliance with data protection regulations concern the rights of the data subject to erasure, rectification and the 'right to be forgotten'.

1.5 Data sovereignty and data ownership

A much-discussed topic of the last two years was what was called data sovereignty which was presented as some kind of counter-concept to traditional data protection – or at least as a further development. The term received considerable attention for the first time at the National IT Summit in 2016. The then Federal Minister for Economic Affairs and Energy, Sigmar Gabriel, said that the

traditional concept of data protection had to be abandoned once and for all because its 'data minimisation' approach stood in the way of modern applications, such as 'big data'. Instead, citizens should be given both physical and legal sovereignty over the handling of data. Federal Chancellor Angela Merkel agreed with this, at least in as far as she said that the idea of data minimisation could no longer be the guiding principle for new products. At this event, none of them explained in more detail what data sovereignty actually means. A glance at the 'Green Paper – Digital Platforms' issued by the Ministry of Economic Affairs suggests that data sovereignty should be tantamount to personal digital autonomy, which, through extensive transparency regulations, is to prevent the information asymmetry which currently often exists in relations between processors and consumers. At the same time, data sovereignty is to enable the commercialisation of data. By and large, however, the more detailed description of data sovereignty presented only shows aspects that are either already regulated under existing data protection law (including the GDPR) or which are not directly related to data protection. The GDPR contains new transparency regulations and provisions regarding data portability, access restrictions for third parties as well as privacy by design and default. The statements in the Green Paper on 'new forms of consent' or on 'differentiated identity management' remain vague. Although the Green Paper addresses possibilities of setting different personal data spheres of data subjects, a central identification database proposed in this context, where data subjects can determine their personal settings for disclosing their data to companies and third parties, poses very specific risks. A central database of this kind would be a paramount point of attack where, in case of doubt, all the personal data of a data subject or even the totality of data entered there could be compromised. Moreover, this centralised collection of personal data would be questionable from a constitutional point of view.

The discussion about the concept of data sovereignty only gained momentum again in mid-2017 when the Federal Ministry of Transport and Digital Infrastructure (BMVI) presented a study on the subject of 'ownership rules for specific mobility data'. Certain concepts of this study also became part of a strategy paper on digital sovereignty issued by the ministry. The concept of data minimisation should be abandoned at this point too. Instead, it should be possible to enhance the commercial usability of personal data, both for companies and for individuals. New value creation opportunities would have to be created for this. Citizens, for instance, should be given the opportunity to decide freely whether they want to disclose data in return for something or whether they prefer to make use of a regular payment option instead. As a precondition for this, it must be possible to create ownership in personal data and to assign personal data to individuals. However, any subsequent use would have to be anonymous and pseudonymised. In the specific environment of modern vehicles, transparency could be achieved in the form of a data passport.

The authors of the study propose several approaches for the concrete implementation of ownership capability, which must necessarily include an exclusive right of disposal:

A data-specific approach where, similar to prior data protection law, the exclusive right lies first with the data subject.

A concrete concept where the exclusive right is based on ownership of the data collection system (example: a monitoring system as part of a vehicle belongs to the vehicle owner who thus also has the exclusive right over the data).

Finally, an action-based approach where the controller of the original data collection has the exclusive right of disposal.

The authors were more open to the action-based approach, whilst the Federal Ministry of Transport and Digital Infrastructure in its strategy paper gave preference to the data-based approach and drew parallels to copyright law. Citizens could therefore transfer some kind of licence to use their data rather than data ownership.

However, both proposals should be viewed critically not only with regard to existing data protection law, but also from the perspective of the constitutionally guaranteed right of informational self-determination.

In the example of mobility, in particular, data would then often be owned by third parties, regardless of whether the person concerned drives or rents the vehicle, since the data subject himself is usually not responsible for the data collection. In case of doubt, the data subject may have no interest at all in the data collection. Instead, vehicle manufacturers or specialised firms would become data owners. In this case, the idea of data as a raw material would be embraced to an unacceptable extent. In the figurative sense, the respective miner would also be the owner of the data gold.

However, personal data is not a commercial object, but always part of a certain natural person whose human dignity is inalienable. The right to informational self-determination also stems from this human dignity. In an action-based approach, these parts of the person would be deprived of the protection of dignity and downgraded to a mere commercial object. However, the idea of humans as a resource is not compatible with our social order. It was not without reason that in 2004 'human capital' was already the non-word of the year and 'human material' the non-word of the 20th century.

Due to the framework set by the right to informational self-determination, it is currently anyway impossible to implement an exclusive right of disposal as a necessary building block of data ownership. Data subjects always have their own rights with regard to their personal data which continue to exist for as long as they can be identified by this data. Whoever owns the data would be deprived of unrestricted control over such data, thus ignoring the very spirit and purpose of ownership. This contradiction becomes particularly clear when looking at data ownership in light of concrete provisions of the GDPR. One example of this is art. 7 (3) GDPR pursuant to which data subjects may withdraw their consent at any time. If the legality of processing depends on that very consent, then no further legal disposal can be made over such data which may be the property of a third party. The effective availability of the 'owner' would be reduced to zero in one fell swoop. These problems apply not only to the action-based approach, but also to the data-specific concept based on copyright law. The granting of a licence by the data subject would also open up possibilities for withdrawing consent or requesting information.

The concept of data ownership as a special form of sovereignty also reveals certain weaknesses. Although data is the raw material of the information society, it cannot be fully compared to the often-cited resources of gold or oil. Whilst unrestricted ownership of these resources is possible without limiting the rights of others, this is often not applicable to data. An inherent feature of personal data is that such data always refers to an individual whose basic interest in being free from observation always plays a role in the handling of that data. Although this fundamental interest can be reconciled with economic interests, which also deserve protection, it cannot be replaced by the latter. An exclusive right to personal data would ultimately depart from the proportional balance between these two interests. In its 2017 Göttingen Declaration on the Value of Data Protection in a Digital Society, the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder comes to the same conclusion: Understood as ownership-like exploitation sovereignty, 'data sovereignty' can only apply in addition to the right to informational self-determination. Even in the digital age, human dignity and the free development of personality remain the yardstick by which state and economic action must be guided. All in all, it can be seen that the debate on data sovereignty does contain some interesting ideas, but it is not very long stone's throw away from 'conventional' data protection law – an observation which is basically already expressed by the term 'sovereignty' itself since this means nothing more than the possibility of self-determination, i.e. the core of data protection law.

1.6 No digitisation in vehicles without sufficient privacy protection

The question of 'data protection in motor vehicles' has been of interest to the media as more and more vehicles offering online services enter the market. This demonstrates the efforts by manufacturers to also provide vehicle users with options for data protection-friendly application.

My colleagues in the Länder and I have repeatedly spoken at the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder about the use of vehicle data in compliance with data protection law. From our point of view, the following key points should be considered:

→ Any data collected during vehicle operation is influenced by the specific use of the vehicle and is therefore personal. This means that there is no data that is irrelevant from the outset under data protection law.

→ The automotive industry is responsible for designing its products in compliance with data protection law and for influencing suppliers and providers of additional services that use the technical vehicle infrastructure in this sense.

→ The automotive industry is hence also committed to the data protection principles of privacy by design and privacy by default.

→ The data collection and processing processes taking place in the vehicle must be fully transparent for vehicle users.

→ Data security and data integrity must be ensured by suitable technical and organisational measures in accordance with the latest state of the art. This specifically applies to data leaving the vehicle.

Dialogue with the German Association of the Automotive Industry (VDA, *Verband der Automobilindustrie*)

The dialogue between the data protection authorities of the Federation and the Länder and the German Association of the Automotive Industry (VDA), which began in December 2014, led to a first result early in 2016 with a joint declaration on aspects of data protection law in conjunction with the use of interconnected and non-interconnected motor vehicles (available at www.datenschutz.bund.de). The manufacturers and suppliers represented by VDA thereby committed themselves to the principles of data protection. They specifically recognise that at least vehicle data associated with the vehicle identification number or the vehicle license plates constitutes personal data. A touchstone for this commitment will be the way in which manufacturers and suppliers comply with their transparency obligations under data protection law and whether vehicle data is in fact collected and processed only with the consent of the owner and, where appropriate, the driver and co-driver. Sovereignty over vehicle data must remain entirely in the hands of vehicle users, whose driving behaviour can be identified from vehicle data. This is what I will support during the further course of the dialogue which will continue in order to address at an early stage the privacy challenges created by the advent of digitalisation in the mobility sector.

Automated and interconnected driving

Digitalisation in the automobile and the transport sector makes cybersecurity and data protection important issues in this area. During the reporting period, I advised the Federal Ministry of Transport and Digital Infrastructure on the amendment of the Road Traffic Act (StVG, *Straßenverkehrsgesetz*) which aimed at allowing automated driving functions for road traffic in Germany. On my initiative, the amount of data to be stored in the car for evidence purposes after an accident was limited to the extent absolutely necessary. Only the loca-

tion and time of the beginning and end of automated driving as well as the location and time of the occurrence of a malfunction may be stored. When the regulation regarding technical details is adopted, I will ensure that the cybersecure technical requirements that protect privacy guarantee state-of-the-art data protection.

In addition, I advise the 'Round Table for Automated and Interconnected Driving' set up by the Federal Ministry of Transport and Digital Infrastructure which brings together representatives from industry, academia, insurance organisations and consumer protection groups. This round table provides first answers to issues that arise from technical developments in order to make automated and interconnected driving systems possible. It is foreseeable that such systems will require the collection and processing of data from a still absolutely unknown quantity of personal data. The necessary legal and technical precautions must be considered at an early stage in order to be able to implement the data protection principle of privacy by design. In this area, the Federal Government has set standards in the energy sector with the Act on the Digitalisation of the Energy Transition (*Gesetz zur Digitalisierung der Energiewende*) which also applies to the automotive and transport sector. One example that deserves special mention is the use of communication components with mandatory security certification, which improve the state of the art for protection against cyber-attacks and uncontrolled data tapping. Even interconnected vehicles should only be able to communicate with other vehicles, the backend systems of manufacturers or third parties, via components that meet the minimum requirements for cybersecurity and data protection defined in a technical guideline designed along the lines of the smart meter gateway for the energy sector.

On 1 June 2017, around 130 guests accepted my invitation and came to Berlin to discuss data protection aspects of automated and interconnected mobility. In a position paper published at the symposium, I gave 13 recommendations for data protection in interconnected and automated vehicles and in digitised transport systems (available at www.datenschutz.bund.de). Data storage, for instance, is usually not required for pure driving operations. If data needs to be exchanged between vehicles, it should be effectively encrypted and protected against unauthorised use. It should also be possible for users to erase personal data unless storage is required by law. These recommendations were included in a decision by the International Conference of Data Protection and Privacy Commissioners made at my instigation at its 39th meeting in Hong Kong from 25 to 29 September 2017 (see also No. 2.5).

Car-to-car communication

In this context, I also address the issue of so-called car-to-car communication. This technology enables vehicles to exchange driving and environmental data via special radio links, for instance, in order to warn each other of road hazards or to independently avoid collisions in intersection areas. The information available to me raises concerns that the principle of data minimisation and data avoidance is not being sufficiently considered during the development of communication standards and the definition of the type and scope of the information to be transmitted. There especially appears to be insufficient provision to ensure that vehicles in the car-to-car network cannot be traced and that personal movement profiles cannot be created on the basis of the travel data exchanged. With this form of online communication between vehicles too, data protection and data

security considerations cannot be separated. Since safety and security of the transport infrastructure are of paramount importance, potential threats must be analysed and technical precautions designed accordingly. Together with my European colleagues, I therefore appealed to the European Commission to adequately consider the requirements of the General Data Protection Regulation when developing rules and regulations for smart transport systems.

Outlook

I am well aware of the positive effects of technological progress in automotive engineering. New systems with a functionality that requires the processing of a large amount of data generated during driving are advantageous for a mobility-dependent society in terms of increased road safety. However, this does not allow industry to neglect its data protection responsibility for the systems it installs. What is important is transparency, data minimisation and maintaining maximum data sovereignty for data subjects.

I am therefore pleased that data protection recommendations are implemented in many newly approved types of vehicles with online data services. Vehicle users can make data protection-friendly settings without having to visit a repair shop. I am confident and will do my utmost to ensure that the cybersecurity of online-enabled vehicles will be guaranteed and can be verified. I am convinced that customers buying a new vehicle will pay attention to its cybersecurity and the possibilities for active data protection and use this as a yardstick for their trust in manufacturers.

1.7 Stronger focus on data protection for children

"I Spy With My Little Eye..."

This was the motto of a conference which I organised for children and media experts at the beginning of July 2018 in co-operation with the Association of Data Protection Officers of Germany (BvD, *Berufsverband der Datenschutzbeauftragten Deutschlands e. V.*), the 'Germany Secure on the Internet' (DSiN, *Deutschland sicher im Netz e. V.*) initiative and the Institute for Media Research and Media Education of the Cologne University of Applied Sciences at the Lower Saxony State Representation in Berlin.

This event, which was attended by around 130 experts from the fields of media education, pedagogy, data protection and politics as well as 70 children and youths aged twelve and over, focused on the question as to what young adolescents themselves think about the topic of data protection, what is important to them and where they would like to see further improvements in light of the media offerings they use every day.

Shortly before the summer holidays, two classes from primary schools in Berlin, supported by 'Germany Secure on the Internet' and the Association of Data Protection Officers of Germany as partners, took an in-depth look at this topic and gave a competent and confident presentation of the results of their workshops at the conference. In the subsequent direct dialogue with the experts, it was possible to shed more light from a data protection perspective on key questions of how minors deal with media offerings, which are often tailored specifically to this group of users, and to highlight the associated problems. It was important to me to experience first hand the thoughts, worries and ideas of children regarding data protection in conjunction with modern media and at the same time to offer them a forum to exchange ideas with experts. This offering was readily taken up and it was impressive to see how the students saw themselves and how critical and sometimes self-critical they were when discussing the topic of data protection in their own environment. The dialogue conference format chosen for this purpose was new for my authority but it proved its worth and is

also suitable for similar events in the future, especially when it comes to specifically addressing and involving children.

One important finding from this conference which I have taken with me is that the issue of data protection should be given even greater prominence in the teaching of digital skills in adolescent education. However, this cannot be left entirely to schools – the private educational environment of children and youths must also be specifically integrated. More information is needed on how, for example, parents or educators in clubs and associations can help prepare children for the risks lurking in the new digital world and sensitise them both to protect their own and to respect each other's personalities. In this context, I have developed a number of recommendations for child-friendly data protection in dealing with digital media (see the recommendations below).

The supervisory authorities of the Federation and the Länder responsible for compliance with data protection regulations also feel committed to these ends. Under the GDPR, they are required to raise public awareness and to provide information, for instance, regarding the risks associated with the processing of personal data. Specific measures for children should also be included in this context. With the 'youngdata' website (https://www.youngdata.de), which has been operated jointly and successfully for years, and the articles and further information on the subject of data protection specially prepared there for children and youths, the supervisory authorities have already established a groundbreaking project in this respect. The importance of this topic has also been recognised by the German legislator and sec. 14 (1) No. 2 of the Federal Data Protection Act expressly assigned to me the task of promoting public awareness and understanding in relation to the processing of personal data, paying special attention to measures specifically for children and youths. The dialogue conference on data protection for children was a first step and will be followed by further specific counselling and information services for children and young adults.

Recommendations of the Federal Commissioner for Data Protection and Freedom of Information for child-friendly data protection in dealing with digital media offerings

Recommendation 1:

Providers of digital media and services which specifically address minors are advised to pay particular attention to the data protection concerns of this target group.

Recommendation 2:

The particular vulnerability of minors must be taken into account by an appropriate design of products and services. Obligations to provide information must be presented in a way children are able to understand.

Recommendation 3:

Media providers and services that either specifically address minors or that at least cannot rule out that their offerings are also used by children and youths under the age of 16 are obliged to ensure comprehensive transparency and security for data processing.

Recommendation 4:

Data protection notices, including information on consents required, must be written in simple language that is easily understood by minors and placed in a clearly visible position.

Recommendation 5:

Parents, teachers and all members of society involved in the care of children and young people are called upon, especially in times of freedom made possible by digitalisation, to raise citizen awareness with regard to both the particular value of personal information and the risk posed by the high vulnerability of their own personality.

Recommendation 6:

Government institutions in particular are responsible for preparing children and adolescents in a comprehensive and age-sensitive manner for the digital world and the risks associated with data protection law, and for informing them about the opportunities and risks of self-aware and critical participation in the diverse media offerings.

Recommendation 7:

At federal and Länder level, associations and institutions should initiate and provide more support for information and education campaigns for child-compliant data protection. This also includes the various initiatives by the data protection authorities of the Länder.

Recommendation 8:

The use of digital media and the imparting of appropriate skills in the field of data protection should be an integral part of school education.

Recommendation 9:

Parents should be supported by information initiatives so that they can provide their children with the necessary assistance, also in the area of data protection, especially during the initial exploration of digital media.

2 Main topics – at European and international level

2.1 The European Data Protection Board

The General Data Protection Regulation established the European Data Protection Board, replacing the former Article 29 Working Party. Its aim is to ensure the uniform application of the General Data Protection Regulation and the Directive on police and judicial data protection (JHA Directive). It has already adopted several guidelines and issued uniform opinions on this subject. One of the main institutional innovations of the General Data Protection Regulation that has been in effect since 25 May 2018 is the introduction of the so-called European Data Protection Board (EDPB). The EDPB is an independent European body which contributes to the uniform application of data protection rules throughout the European Union and promotes co-operation between EU data protection authorities. The Board performs its duties and exercises its powers independently and not subject to any instructions. Just like its predecessor, the so-called Article 29 Working Party, the Board is composed of the heads of the EU data protection supervisory authorities of the EU Member States and the European Data Protection Supervisor. The supervisory authorities of the EEA states are also members with regard to matters relating to the GDPR, however, without voting rights and without the right to be elected Chairperson or Vice-chairperson. The European Commission is entitled to attend Board meetings without the right to vote. The Board is represented by a Chair elected for a term of five years. On 25 May 2018, Dr Andrea Jelinek, head of the Austrian data protection authority, was elected as the first Chairperson of the Board. The Board has its seat in Brussels.

EU Member States, such as Germany, which have several national supervisory authorities, must appoint a 'joint representative' for the EDPB. The Federal Data Protection Act delegates the function of joint representative to the Federal Commissioner for Data Protection and Freedom of Information (BfDI). At the same time, the Federal Commissioner for Data Protection and Freedom of Information acts as a 'single point of contact' and enables the supervisory authorities of the other Member States, the EDPB and the European Commission to effectively communicate with German supervisory authorities without knowledge of the national distribution of responsibilities. The Bundesrat elects a head of the data protection supervisory authority of a Land as the joint representative's deputy.

The EDPB is tasked with ensuring the uniform application of the GDPR and of the JHA Directive within the EU and, for this purpose, is assigned a comprehensive range of tasks under the GDPR and the JHA Directive. The EDPB has an advisory function with regard to data protection policy and data protection law at EU level, especially with regard to legislative proposals by the European Commission. The Board can also develop guidelines, recommendations and best practices concerning data protection issues, such as data processing in conjunction with profiling, certification procedures and privacy seals or data transfers to third countries. The EDPB has a special task within the framework of the so-called consistency mechanism (art. 63 et seqq. GDPR). The purpose of this procedure is to harmonise the application of the law and the supervisory practice of the data protection authorities of the Member States. Within this procedure, the Board can, for example, give its opinion if a national authority wishes to approve binding data protection provisions for international data transfers within a group of companies (so-called Binding Corporate Rules, see No. 17.8.1 below). The Board also makes legally binding decisions on the question as to whether there has been a violation of the GDPR if the data protection authorities concerned in the Member States cannot agree on a uniform view. However, such a dispute settlement procedure has not yet taken place within the reporting

period.

Just like the Article 19 Working Party, the EDPB can also resort to expert groups which prepare the Board's comments and decisions on specific issues.

The Board is supported by a secretariat in charge of administrative issues, whose staff is provided by the European Data Protection Supervisor (EDPS) and experts from the national supervisory authorities. The secretariat's staff are subject exclusively to instructions by the EDPB Chair and are organised separately from the EDPS in this respect. In addition to providing administrative support to the Board, the secretariat prepares draft opinions and other EDPB documents in accordance with instructions from the Chair including draft binding decisions within the consistency mechanism.

Within the reporting period since the coming into effect of the GDPR, the EDPB has adopted guidelines on the geographical scope of application of the GDPR (art. 3 GDPR), on certification (art. 42 GDPR) and accreditation (art. 43 GDPR) as well as on exceptions for data transfers to third countries (art. 49 GDPR). The EDPB has also issued uniform opinions on lists of data processing operations for which data protection impact assessments must be carried out pursuant to art. 35 GDPR in measures pursuant to art. 64 GDPR. It has also confirmed various guidelines relating to the GDPR which were still adopted by the predecessor body, i.e. the Article 29 Working Party, including the lead supervisory authority, consent (art. 6 GDPR), the right to data portability (art. 20 GDPR), the data protection officer (art. 37 GDPR), data protection impact assessments (art. 35 GDPR) and profiling (art. 22 GDPR). Finally, the EDPB adopted an opinion on the European Commission's draft adequacy decision on Japan (see No. 2.1.1).

The guidelines and other documents adopted by the EDPB are available at www.datenschutz.bund.de.

2.1.1 International data traffic

During the period under review, the debate on international data traffic was once again marked by adequacy decisions adopted by the European Commission.

Adequacy decision on Japan

Just like under the European Data Protection Directive 95/46/EC, the European Commission can decide under art. 45 GDPR that a country that is not bound by the data protection provisions applicable in the EU offers an adequate level of protection.

Personal data from the EU may then be transferred to that country without further protection measures. In September 2018, the European Commission submitted a draft of such an adequacy decision on Japan and finally adopted this on 23 January 2019. On 5 December 2018, the EDPB delivered its opinion pursuant to art. 70 (1) (s) GDPR on this draft. My authority played a major role in the preparation of this opinion. After the reform of Japan's data protection law, the EDPB sees major parallels to the European data protection regime and recognises that the additional rules adopted for data transferred from the EU contribute significantly to the protection of data subjects. Although the European Commission has modified and improved its draft adequacy decision in light of the EDPB's suggestions, the EDPB still calls for increased monitoring of certain areas in practical life. The focus will be specifically on questions relating to the informativeness of consent, which is a central legal basis for data processing under Japanese law, on the further transfer of European data to third countries and on access by security authorities to data transferred from the EU to Japan on the basis of the adequacy decision. The EDPB also believes that further improvement is required with regard to the existing possibilities for EU citizens to obtain remedy in the case of data protection breaches by Japanese data controllers.

EU-US Privacy Shield

As described in my 26th Activity Report

(No. 2.1), the EU-US Privacy Shield (Privacy Shield) has since 12 July 2016 provided a legal basis for data transfers to the US in the form of an adequacy decision, which, however, the European data protection authorities still regard this with concern. The Privacy Shield underwent two joint reviews during the reporting period, in which I was extensively involved. The clear criticism of the Article 29 Working Party before and after the first joint review, which was confirmed by the EDPB in July 2018, led to improvements in the privacy shield. When the second joint review took place in October 2018, it was noted that the certification process and the procedures to implement the Privacy Shield had been strengthened: The missing members of the Privacy and Civil Liberties Oversight Board (PCLOB), which oversees US security agencies, were appointed and a previously classified report of that board was published. However, the EDPB still has concerns, especially with regard to the ombudsperson. This post has not been permanently filled since the beginning of the Trump administration. Although the US government has meanwhile nominated an ombudsperson, this has not yet been confirmed by the US Congress. The question as to whether the ombudsperson can actually guarantee effective legal protection within the meaning of art. 47 of the Charter of Fundamental Rights of the European Union remains open and was referred to the European Court of Justice for clarification. This procedure and a further case against the Privacy Shield pending before the European Court of Justice will shed further light on the framework conditions for transatlantic data traffic and data transfers to other third countries.

2.2 Participation in data protection supervisory groups

European Visa Information System

Since October 2011, the European Visa Information System (VIS) has been on stream and is subject to Community supervision by an existing data protection supervisory group at EU level. The group has issued a critical opinion regarding the European Commission's draft for a new VIS Regulation.

As a common European database, the purpose of the VIS is to avoid the double issuance of short-term visas and to facilitate cooperation between the participating states within the framework of a common visa policy. In line with the tried-and-tested architecture of large European databases, the VIS consists of a central unit operated by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) in Tallinn and the national components of the participating states.

At the end of the reporting period, the EU Member States, with the exception of the UK, Ireland, Bulgaria, Romania, Croatia and Cyprus, but supplemented by Norway, Liechtenstein, Iceland and Switzerland, participate in the European VIS as part of the 'Schengen acquis'.

The data protection supervision of the VIS is based on the model of coordinated control: The European Data Protection Supervisor controls the central VIS database, whilst the data protection authorities of the Member States check the respective national components of the VIS. In Germany, I am responsible for data protection control because the Federal Foreign Office and the Federal Office of Administration are responsible for the application of the VIS. In order to coordinate the work and control priorities in the Member States, a joint data protection supervisory group – currently chaired by Switzerland – was set up and meets at least twice a year. I regularly participated in the deliberations and activities of this group.

During the reporting period, the group developed procedural principles on how the supervisory activities of national supervisory authorities pursuant to art. 41 of the European Regulation 767/2008 (VIS-Regulation) are to be exercised. It also adopted a position paper on the use of external service providers to process visa applications at diplomatic missions and consular offices of the Member States.

With a view to the European Commission and the Council's objective of closer interconnecting existing and new databases of the European Union (so-called interoperability), the group adopted a joint opinion with the relevant supervisory groups of Eurodac (see below) and the Schengen Information System.

At the end of the reporting period, the revision of VIS Regulation was not yet finalised. The draft presented by the European Commission provides, for instance, for a reduction in the minimum age of children whose fingerprints are taken from 14 to six years. Moreover, security authorities will have extended access to the data stored in the VIS. The scope of the VIS will be generally expanded by including longer stay visas (more than 90 days) and residence permits as well. The data protection supervisory group sent a critical opinion on these and other aspects to the European Commission, the Council and the Parliament because the group feels that the need for this extended intervention in the right to informational self-determination of data subjects has not been sufficiently demonstrated.

The opinions on the Eurodac, Schengen and VIS interoperability project and on the European Commission's draft new VIS Regulation are available on my website atwww.datenschutz.bund.de .

Eurodac

Fingerprints of asylum seekers are stored in the European 'Eurodac' database. The competent data protection supervisory group carried out investigations, for instance, into the rights of data subjects. The name 'Eurodac' refers to a common database for fingerprints of asylum seekers and illegal immigrants apprehended in the EU. The database supports the effective application of the Dublin Convention on the processing of asylum applications. Eurodac was established on the basis of an EU Council Regulation, which also includes rules guaranteeing data protection for the individuals concerned. The database went live on 15 January 2003 and is currently used by the 28 EU Member States as well as Iceland, Norway, Liechtenstein and Switzerland.

The European Data Protection Supervisor (EDPS) supervises the processing of personal data in the central system of the database, including data transfers to the Member States. The data protection authorities of the Member States supervise the processing of data by the national authorities and the transfer of such data to the central system. In order to ensure a common approach to data protection control, representatives of the EDPS and supervisory authorities from the user countries meet at least twice a year in the Eurodac Supervision Coordination Group which is currently chaired by Sweden. I regularly take part in the consultations and activities of this group.

During the reporting period, the joint group conducted a coordinated study on how to ensure the protection of data subjects' rights in the Eurodac user countries. A report with recommendations is expected to be published in 2019. The group also continued its work on the advance erasure of fingerprints in Eurodac (art. 13 of Regulation (EU) 603/2013) and the report on this issue is also likely to be published in 2019.

2.3 Finalisation of the revision of Convention 108 on data protection

The globalisation of data traffic not only required modernisation of the European Union's data protection legislation. Since 2009, the Council of Europe has also been working on the revision of the 1981 Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108). The protocol of amendment was adopted by the Council of Ministers of the Council of Europe on 18 May 2018.

Convention 108 of the Council of Europe dates from 1981 and was the first legally binding intergovernmental convention on data protection. It lays down the main principles of data protection law and applies to both the private and public sectors.

In view of enormous technological developments, it was necessary to modernise Convention 108, including its amending protocol of 2001. The process extended over a term of several years and was successfully completed in May 2018 with the adoption of the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. During the development process, I attended the meetings of the Consultative Committee (art. 18 of the Convention). In addition to the 47 Member States of the Council of Europe, which includes all the EU Member States and a number of other countries, such as the Russian Federation, Turkey, Switzerland and Norway, the countries of Uruguay, Mauritius, Senegal, Tunisia, Cape Verde and most recently Mexico have also ratified Convention 108. Convention 108 is thus of significance, far beyond Europe, for the global development of data protection law.

The Protocol of Amendment aligned Convention 108 (i.e. the basic principles of data protection law, the rights of data subjects and the obligations of the data controller) with the principles of the General Data Protection Regulation, so that the necessary coherence between the Convention and the new EU legal framework could be achieved. The signatory states are especially obliged to strengthen the rights of data subjects. They are, for instance, to be given the right to gain knowledge of the way in which data is processed and to object to it.

Furthermore, a provision must be introduced under which data controllers have an obligation to report to the supervisory authority if data protection violations have occurred. The creation of independent supervisory authorities with the power to control and sanction data breaches and to co-operate with each other for the purposes of implementing the Convention is also mandatory for all Convention States.

2.4 European Data Protection Conference

In 2017 and 2018, the annual Spring Conference of the European Data Protection Supervisors focused on developments concerning the implementation of the General Data Protection Regulation and the modernisation of Convention 108, as well as the supervisory powers of data protection authorities. At the European Data Protection Conference, representatives of all data protection supervisory authorities in Europe, the European Commission, the Council of Europe and the OECD came together to exchange views and experiences.

At the 2017 Spring Conference in Limassol (Cyprus), the question as to how awareness can be raised among citizens and companies for the effective protection of personal data was discussed in addition to issues regarding the implementation of the GDPR. The participation of consumer protection associations as multipliers and the role of in-house data protection officers were also discussed. A discussion on cloud computing also addressed transparency obligations and responsibility on the part of operators.

The 2018 Spring Conference was held from 2 to 4 May 2018 in Tirana (Albania) under the title “Data Protection – Better Together”. Several forums addressed, among other things, the implementation of the GDPR, the modernisation of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108, see No. 2.3 above) and its influence on data protection worldwide.

The challenges and opportunities in dealing with data protection violations on social media platforms were discussed with reference to the ‘Cambridge Analytica – Facebook’ case. The discussion on the powers of the respective supervisory authorities highlighted the considerable differences that still exist between the members. The conference also discussed the question of the ethically justifiable use of artificial intelligence in the police and judicial sector, including the monitoring of the use of such technology in this sector (see also No. 1.4 et seq.).

The texts of the resolutions of the 2017 and

2018 Spring Conferences are available on my website at www.datenschutz.bund.de .

2.5 International Conference of Data Protection and Privacy Commissioners

The International Conference of Data Protection and Privacy Commissioners addressed important topics for the future. It passed decisions on interconnected driving and on the data protection challenges that can arise from the development and use of artificial intelligence.

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Hong Kong (25 to 29 September 2017) was held under the motto "WE – Connecting West with East in Protecting and Respecting Data Privacy". This motto was to reflect that the protection of personal data must be an international task. Three resolutions were adopted at the conference. Besides the two resolutions on internal co-operation between members of the ICDPPC and on co-operation with consumer protection authorities, special mention should also be given to the resolution on "the protection of personal data in automated and interconnected vehicles", which I was able to submit to the conference together with data protection supervisory authorities from Belgium, France, Italy, Hong Kong, Mexico, New Zealand, Slovenia, Switzerland and the United Kingdom. The Resolution calls on all interested parties, most notably standardisation bodies, public authorities, vehicle and equipment manufacturers, private transport and car rental companies, as well as providers of data-driven services, such as voice recognition, navigation, remote maintenance or telematic services for motor insurance, to fully respect the fundamental rights of users to protection for their personal data and privacy and to take these fundamental rights sufficiently sufficiently into account at every stage of the production and development of new devices or services. For this purpose, 16 concrete requirements are subsequently laid down in the resolution (see also No. 1.6).

The 40th ICDPPC in Brussels and Sofia (21 to 25 October 2018) entitled "Debating Ethics: Dignity and Respect in a Data Driven Life" was organised by the European Data Protection Supervisor together with the Bulgarian Data Protection Authority. The discussions focused on the challenges which current developments in certain future technologies pose for the protection of the individual's privacy and for ensuring data protection. In view of the very serious consequences that artificial intelligence applications (see No. 1.4 et seq. above) can have, the ICDPPC adopted a "Declaration on Ethics and Data Protection in Artificial Intelligence". It expressed its view that the creation, development and use of artificial intelligence systems must fully respect human rights and, in particular, the right to the protection of personal data and privacy, human dignity, non-discrimination and fundamental values, and that solutions must always be provided that enable individuals to maintain control over and understand artificial intelligence systems. To this end, the Conference adopted six guiding principles: (1) fairness, (2) continued attention and vigilance, (3) transparency and intelligibility, (4) privacy by design and privacy by default, (5) empowerment of every individual, and (6) avoidance of bias and discrimination. In keeping with its motto, the 40th ICDPPC also discussed whether and to what extent ethical and moral values can serve as a basis for ensuring data protection even under the conditions of the digital age and whether these values are suitable instruments for overcoming the challenges facing data protection as a result of new forms of interaction between humans and machines – such as artificial intelligence applications – and ever-faster technological progress. It goes without saying that the conference was merely the starting point for this debate. Future ICDPPC conferences will have to continue this debate and supplement the data protectors' 'toolkit' with universally applicable, ethical and moral principles for dealing with future technologies.

The resolutions adopted by the International Conference of Data Protection and Privacy Commissioners are available in

English on my website (www.datenschutz.bund.de) where working translations of the resolutions are also available in German.

The 41st ICDPPC will be held from 21 to 25 October 2019 in Tirana, Albania.

3 Labour and social affairs committee

3.1 From the legislative projects

3.1.2 European Social Fund

The EU Regulation on the European Social Fund Plus (ESF Regulation) is the result of the merger of the European Social Fund (ESF), the Youth Employment Initiative, the Fund for European Aid to the Most Deprived, the EU Programme for Employment and Social Innovation (EaSI) and the EU Health Programme. The proposed regulation does not meet the requirements of the GDPR. In my 25th Activity Report, I already reported on the ESF, the large number of bodies involved in the funded projects and the related data processing issues (see No. 9.4).

Discussions are currently underway at EU level in order to prepare the next 2021 to 2027 funding period for projects to be supported by ESF+ funds. According to the draft Regulation, personal data is to be collected primarily from registers, comparable sources or 'informed estimation' for verification purposes. In my opinion, the design proposed for this procedure does not comply with data protection law. The way in which data is processed is contrary to the purpose of the original data stored in registers. It also makes it more difficult for people participating in ESF-funded projects to exercise their rights as data subjects.

I therefore support the Federal Ministry of Labour and Social Affairs in its effort to urge the European Commission to design the procedure in a way that complies with data protection requirements.

6 Finance committee

6.1 From legislation

6.1.1 New task for the Federal Commissioner for Data Protection and Freedom of Information (BfDI)

Since 25 May 2018, I have been in charge of data protection supervision tasks also for the revenue authorities of the Länder, including the revenue offices and parts of the municipal tax offices. With the Act amending the Federal Law on War Pensions and Other Regulations (*Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften*) of 17 July 2017 (Federal Law Gazette I 2017 p. 2541), which came into effect on 25 May 2018, I was assigned the task of supervising data protection at the revenue authorities with regard to the processing of personal data within the scope of the Fiscal Code of Germany (AO, *Abgabenordnung*) pursuant to sec. 32h (1) AO. As far as the municipalities are responsible for handling property taxes, i.e. business and real estate tax, I was also made responsible for supervising data protection at municipal tax offices via the corresponding reference in sec. 1 (2) No. 1 AO. Finally, pursuant to sec. 32h (3) AO, a decision can be made under Länder law to delegate to me the supervision of the processing of personal data within the framework of Länder or municipal tax laws if data processing is based on tax bases regulated by federal law or on uniform federal provisions. The Free and Hanseatic City of Hamburg was the first Land to make use of this opportunity.

Even before the new regulations came into effect, I had worked extensively at administrative level in order to ensure that this transfer of responsibilities from the data protection supervisory authorities of the Länder to my organisation went smoothly. I supported and advised, for example, the respective working groups and working teams of the Federal Ministry of Finance and the supreme fiscal authorities of the Länder in numerous discussions and voting rounds. This consulting activity concerned both my new supervisory responsibility and the implementation of the requirements under the GDPR by the revenue authorities.

Consultation

During the reporting period, I paid a first fact-finding visit to a supreme finance authority of a Land and two revenue offices. Numerous operational issues were clarified, but also questions in conjunction with the required appointment of a data protection officer. During my visits to the two revenue offices, I was able to convince myself that they handle the tax data of their citizens carefully and in compliance with data protection regulations. Moreover, during the short time of my new supervisory responsibility, I already received and have followed up on numerous inquiries from citizens.

Moreover, both the Federal Ministry of Finance and the supreme revenue authorities have asked me for advice on individual issues. It was, for instance, possible to clarify that wage tax assistance associations as non-public bodies are subject to the data protection supervision of my colleagues in the Länder. The same applies to tax advisors.

6.2.1 International tax data exchange

On 29 October 2014, 51 states signed an agreement in Berlin on the automatic exchange of information in tax matters, the so-called OECD standard. Up to now, 104 states have acceded to the agreement. The first data exchange between the original 51 signatory states took place in September 2017. At the level of the Organisation for Economic Co-operation and Development (OECD), a joint initiative with the G20 States and in close co-operation with the EU, a model for the Standard for Automatic Ex-

change of Financial Account Information in Tax Matters was developed. This provides that the competent government bodies receive the necessary information from the financial institutions and automatically exchange it with other states once a year. On 29 October 2014, 51 states signed a multilateral agreement on this standard. Within the framework of national implementation, I tried to work towards a solution in conformity with data protection law, but did not succeed in all respects (see 25th Activity Report No. 7.9; 26th Activity Report No. 8.2.4).

The first exchange of information between the 51 early adopters took place in September 2017.

I followed the issue through the Article 29 Working Party and the European Data Protection Board (EDPB) and I am in dialogue with the OECD via the Financial Matters Subgroup of the EDPB. The EDPB had prepared a questionnaire in order to survey the state of implementation of the OECD standard in the member states at the national ministries of finance and to gather experience with the first data exchange in September 2017. A positive takeaway from the replies is that no serious data breaches have occurred so far.

7 Health committee

7.1.1 General Data Protection Regulation in medical research and the health sector

The legislator must guarantee the necessary protection of health-related and genetic data even in the context of research using such data. In my 26th Activity Report, I already pointed out that the digitisation of the healthcare system and rapid technological development promise new opportunities for research with health-related and genetic data, for which the GDPR now sets the framework conditions (see No. 9.1). Since the GDPR came into effect, there has been no significant experience in the field of medical research, but some uncertainty exists with regard to the legal basis for research activities. The provisions of art. 89 GDPR can be interpreted as rather research-friendly in light of the EU's general position on science and the objective of creating a European research area as laid down in art. 179 of the Treaty on the Functioning of the European Union (TFEU). Notwithstanding this, we must not lose sight of the protection of data subjects, especially in the case of sensitive health-related and genetic data.

The new version of sec. 75 Tenth Book of the Social Code (SGB X, *Zehntes Buch Sozialgesetzbuch*) is of particular importance with regard to the adaptation of the provisions on social data protection in the Tenth Book of the Social Code (see No. 3.1.1). This section lays down rules for the entitlement of social service providers to make social data available for scientific research purposes (see also 25th Acivity Report No. 9.5). This data is to a large extent health data. The previous rules for the obligation to approve the provision of social data for scientific research purposes as well as the restrictions on the processing of this data for certain research projects in the area of social benefits or scientific labour market and occupational research have been basically retained. I also expressly welcome the fact that the requesting social service provider must submit a data protection concept for the research project. This makes it easier for both the approval and the data protection supervisory authority to review the research project and ultimately ensures better protection of sensitive social data.

However, a new provision for follow-up research was introduced in subsection 2. According to this provision, the period given to researchers to process social data for research purposes may either be extended or completely redefined and further social data may be transmitted if scientific research raises a further research question related to the content of the original research question. A simplified approval procedure will then also apply if social data transmitted on the basis of the original approval is to be used for other, however, more far-reaching new research questions related to the original research question. The provision leaves room for misleading interpretation and the way approval authorities interpret the standard will have to be monitored.

I am particularly critical of sec. 75 (4) 6th sentence SGB X which combines two different provisions in one sentence. The ten-year retention period from the first part of the sentence serves to enable the reproduction of research results. This is the result of a demand by the German Research Foundation (DFG, *Deutsche Forschungsgemeinschaft*) and a response to fraudulent scientific publications in the 1990s. There are no concerns against this provision from the point of view of data protection law. However, it must be stressed that the very purpose of the provision requires that the raw data underlying the scientific research results may not be altered so as to prevent manipulation. However, this is contradicted by the provision in the second part of the sentence pursuant to which this data, which is to be used exclusively for the purposes of verifying research results, is available for further research. Sec. 75 (4) 6th sentence SGB X thus creates the impression that its intention is to leave sensitive data to the free disposal of research irre-

spective of a specific research purpose. This goes far beyond what would even be permissible under the so-called 'broad consent' in recital 33 of the GDPR. Here, too, the yardstick must be the principle of necessity. I am concerned that the GDPR, despite all the privileges granted to scientific research, is based in principle on the informed consent of data subjects when they make their data available for scientific research, whilst provisions such as sec. 75 (4) 6th sentence SGB X make the reference to 'broad consent' the rule. The idea of 'broad consent', i.e. consent for research purposes not yet sufficiently established at the time of consent, was only introduced into the GDPR in the very last late phase of the so-called trilogue on what later became recital 33. The actual text of the norm only contains provisions regarding informed consent of the data subject.

The Article 29 Working Party also pointed out in its opinion on consent that "recital 33 does not eliminate the obligations relating to the requirement of consent for the particular case". This means that scientific research projects may in principle only include personal data on the basis of consent if the purpose is precisely described. In cases where it is not possible at the beginning to specify the purposes of data processing within the framework of a scientific research project, recital 33 exceptionally allows the purpose to be described in a more general way (Working Paper (WP) 259 rev. 01 of 10 April 2018, p. 34). 'Broad consent' is hence an exception which, in accordance with the generally applicable rules of legal interpretation, must be interpreted in the narrow sense.

Unfortunately, my objections to the amended sec. 75 SGB X were not taken into consideration also with a view to the procedure chosen by the Federal Government to introduce this in the form of formulation aids in the parliamentary deliberations on the Federal Law on War Pensions and Other Regulations (see No. 3.1.1). For example, other, much more data protection-friendly consent models have not been sufficiently discussed. This includes, for example, the internationally discussed 'dynamic consent' where the data subject has the option of granting, withdrawing or modifying their consent to individual parts throughout the course of a scientific study. In social science studies in the US and the UK, this has already been achieved using a corresponding app.

I will also keep an eye on the use of personal data, in particular, health-related data, outside the field of research involving social data. I would like to stress here that I have a very positive attitude towards scientific research. However, in the scientific evaluation of personal data, it should not be forgotten that it is not only science that can claim freedom of research. Data subjects whose data is used for scientific purposes also have fundamental rights. I will be glad to continue providing my expertise here in order to enable appropriate results in the balance between freedom of research on the one hand and the right to informational self-determination on the other.

7.1.2 Electronic health and medical records as well as so-called health apps

A confusion of terms can also lead to harmonisation.

The press repeatedly reports on 'electronic health records' or the 'electronic medical record'. The statutory health insurance funds are beginning to offer policyholders a possibility to store and electronically access their health data. The Federal Ministry of Health is also driving developments in the field of digitalisation in the healthcare sector, which I am also working on due to the associated data protection issues.

The general public makes little or no distinction between the different solutions for health data collection. The terms 'medical record' and 'health record' are used synonymously. It is, however, important to know that the different solutions are based on different legal bases and have different consequences, especially for policyholders (see chart for No. 7.1.2).

Electronic medical record

The term 'electronic medical record' is used both in the German Civil Code (BGB, *Bürgerliches Gesetzbuch*) and in the Social Code (SGB, *Sozialgesetzbuch*). What the electronic patient record has in common according to both sec. 630f BGB and sec. 291a of the Fifth Book of the Social Code (SGB V, *Fünftes Buch Sozialgesetzbuch*) is that it is to be kept by service providers (physicians, psychotherapists, pharmacists, hospitals, etc.). It contains findings, diagnoses, treatment reports, etc. and documents medical treatment just like the previous printed patient record. In the case of the electronic patient record within the meaning of sec. 291a SGB V, it must also be considered that it is basically designed to be cross-institutional rather than case-related.

According to the current legal framework, the electronic patient record is to be supported by the electronic health card as contemplated in sec. 291a SGB V. Access to the data requires an electronic health professional card as well as an electronic health card with proof of the policyholder's consent. In the same way, policyholders can also make their data available to certain service providers. In contrast, the electronic patient record according to sec. 630f BGB is the implementation of the medical documentation of the treatment which only the treating and documenting physician can access.

Electronic health record

There is no binding definition for the electronic health record. Instead, it evolved from the possibility for statutory health insurers, as laid down in sec. 68 SGB V, to financially support their policyholders in the use of an 'external' electronic health record. Unlike the electronic patient record, which is kept by the respective service provider for documentation purposes, the electronic health record is sometimes developed by private companies in close co-operation with statutory and private health insurers and offered as part of a 'health app'. As with an electronic patient record within the meaning of sec. 291a SGB V, the health-related data of the policyholder can be collected, processed and stored. However, this is basically independent of the telematics infrastructure and hence does not use the electronic health card.

There are no fundamental data protection concerns about the electronic health record or the electronic patient record. However, problematic data protection issues were found in several audited projects. This applies, for example, to the authentication process or to the transfer of user data by tracking services. The planned electronic transmission of certificates of incapacity for work outside the telematics infrastructure system is also questionable under data protection law. I am also sceptical about the possibility of sending health-related data within the meaning of sec. 305 SGB V directly from the health insurance company to an electronic health record. Due to the narrow interpretation of sec. 284 SGB V, the statutory health insurance funds are not entitled to transmit this data to anyone other than the policyholder. This even applies when consent has been given by the data subject. However, the draft Appointment Service and Medical Care Act (TSVG, *Terminservice- und Versorgungsgesetz*) which was still under parliamentary consideration at the time of the copy deadline will create a corresponding legal basis.

Within the scope of the Appointment Service and Medical Care Act, access to the data of the electronic patient record will be possible in future even without a health professional card. Up to now, the legislator's concept also provided for an electronic patient postbox in addition to the electronic patient record. The different access rules for this electronic patient postbox differ from those for the electronic patient record.

With the coming into effect of the Appointment Service and Medical Care Act, however, the legislator plans to merge the electronic patient postbox with the electronic patient record and standardise it. The previously planned patient postbox will then be omitted.

In compliance with data protection requirements, the use of electronic patient and health records requires further legislation and framework conditions. In this context, special importance must be attached to ensuring that data sovereignty clearly remains with policyholders. In addition, the voluntary nature of the use of such a 'health data collection' must be warranted.

Health apps

In my 26th Activity Report (No. 1.5 and 9.2.4), I already reported on data protection issues in conjunction with the so-called health apps. Unfortunately, these problems continue to exist. Furthermore, access to electronic health records is increasingly being based on so-called health apps. In the summer/autumn of 2018, for instance, there was extensive press coverage on the app from the company Vivy GmbH. The security of the Vivy app is being examined by the Berlin Commissioner for Data Protection and Freedom of Information.

The use of mobile applications, including health apps in the field of health care, is also the subject of a report issued by a working group in which I participate and which was set up by the Federal Ministry of Health.

7.1.3 Electronic health card – state of an eternally unfinished procedure

As reported in the last Activity Report, testing of the electronic health card at doctor's offices has finally begun, but first medical applications are still missing.

Even the policyholder master data service has not yet been put into operation. Patients still have to wait. In my 26th Activity Report, I reported on the planned testing measures in the Northwest and Southeast test regions (see No. 9.3.2). However, progress is very slow.

But the noticeable revival of the electronic health card project through the Act for Secure Digital Communication and Applications in Health Care (E-Health-Gesetz, *Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen*; see 26th Activity Report No. 9.2.1) is taking effect. Technical concepts for the first applications (emergency data management, electronic patient record) are now available or are about to be finalised. The threat of sanctions seems to be making an impact.

In 2019, the electronic health card will finally go live. The policyholder master data service and emergency data management will be the first applications to be supplemented by the electronic patient record (ePA) by mid-2019 (see also No. 7.1.2). The necessary medical profession cards for physicians as well as institute cards are now being issued.

After application of the GDPR began in May 2018, the question arose as to who is actually responsible for the telematics infrastructure (TI) and thus has to submit a data protection impact assessment (DPIA) (see also No. 15.2.3). Many doctor's offices have fulfilled their legal obligation to prepare a DPIA. However, they did not stop at the threshold of their practice rooms, but also included the TI in their considerations. The DPIA that is prescribed by law for doctor's offices then showed that connection to the TI was not justifiable. Many physicians thus approached me on this matter.

The question as to who is the controller within the meaning of the GDPR and hence responsible for the TI was not finally answered by the copy deadline.

7.1.5 Use of messenger services by social security institutions

The offer by several social insurance organisations to contact their policyholders via messenger services is problematic from the perspective of data protection law. This specifically applies to the most widespread messenger, WhatsApp, which regards its use as 'consent' even to non-transparent data transmission to Facebook and to regular address book uploads (regarding general issues of data protection problems with mes-

senger services, see No. 15.2.6). Since health-related data, which belongs to the special categories of personal data pursuant to art. 9 (1) GDPR and therefore enjoys particularly high protection, can often be involved in contact with social security institutions, I drew the attention of social security institutions to the fact that alternative communication procedures should currently be used due to a lack of data protection conformity.

9 Committee on Home Affairs and Community

9.1 From the legislative projects

9.1.3 The country needs new police laws – but which ones?

After the Directive on police and judicial data protection (JHA Directive) came into effect in 2016, legislators at federal and Länder level became active. In my last Activity Report, I already reported on the new Federal Criminal Police Act (BKAG, *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*) which is now in effect. However, one should not forget that internal security actually lies within the competence of the Länder. The Federation has only a supplementary function and the Federal Criminal Police Office merely a coordinating function. Although the Federal Police Act (BPolG, *Gesetz über die Bundespolizei*) was amended, the Directive was not transposed into national law. A corresponding draft was announced for the beginning of 2019.

Federal Criminal Police Act – a short gleaning

The new Federal Criminal Police Act came into effect in May 2016 (see 26th Activity Report No. 10.2.9.1). It was pushed through under enormous time pressure, so that little time was spent on detailed deliberations of its content by parliament.

Especially the new information system that was determined against my advice – a central information system was already permitted under the old law – was presented as highly urgent during the negotiations. It is therefore all the more surprising that it is now suddenly no longer so urgent in practice (see No. 9.2.4). The Act did at least address my demand that the so-called automatic drag-along mechanism in conjunction with deadlines for the examination of the need to erase incorrect or unlawfully transmitted data (see also 26th Activity Report No. 10.2.9.1) be omitted.

The police authorities of the Länder need the Federal Criminal Police as a well-functioning central institution which must coordinate and, where appropriate, work towards a targeted, effective exchange of information between the competent police authorities to these ends. This is also unobjectionable from a data protection perspective. But one should not forget that the tasks of the central institution are limited (see also No. 9.3.6 et seq.). The Länder remain responsible for threat prevention. It is therefore questionable also from a data protection perspective if more and more tasks and powers are to be transferred to federal authorities. This will lead to more data being processed at a central location. However, security is not mainly produced by the Federation and above all not by extensive central databases. The general question is: Will new and more comprehensive powers lead to greater security? Far too little attention is being paid to the question as to whether the police authorities are well positioned in practice or whether enforcement deficits exist. Legislative actionism is of little use here.

The Federal Police Act

The JHA Directive has not yet been transposed for the Federal Police, so that the transposition deadline was missed. Although a corresponding draft was announced, it was not yet available by the copy deadline.

However, the Federal Police Act was amended by the Act to Improve Investigation in Particular Hazard Situations and to Protect Civil Servants of the Federal Police (*Gesetz zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei*). This act introduced the so-called bodycam for federal

police officers. In this context, some of my remarks were taken into account in the deliberations by the department. The following point, for instance, was important to me: If the cameras are used, this should be not only to the disadvantage of the individuals concerned, but also to their benefit. The data collected cannot only be used for criminal prosecution. Citizens affected by measures may also request that the recordings be used to check the legality of police operations. I also criticized the location where the Federal Police store and process the bodycam data. The data is stored and processed on cloud servers of a US company. In this case, the Federal Police do not have an exclusive right to issue instructions to the processor under the United States Act (*Clarifying Lawful Overseas Use of Data Act*). It is possible for US authorities to demand the surrender of data. Only the cloud provider and not the Federal Police who are responsible can contradict to this. US courts then decide on the protest. This does not correspond to the clear requirements for processing carried out on behalf of a controller pursuant to sec. 62 of the Federal Data Protection Act (BDSG, *Bundesdatenschutzgesetz*) and is therefore unlawful. I repeatedly pointed this out to the Federal Police (see also No. 9.3.3).

Another new feature is license plate recognition which can, for instance, be carried out if a risk of serious near-border or cross-border offences exists. In this area, in particular, I expressed doubts as to whether a sufficient time restriction is ensured for the measures to be taken. The risk is therefore that a measure will be established permanently. Furthermore, it is not clear against which search database the data can be checked. Especially in this area, the Federal Constitutional Court called for legal clarification.

9.1.4 New Customs Investigation Act

The provisions of the Directive on police and judicial data protection (JHA Directive) should have been implemented by 6 May 2018 for the Customs Investigation Service (see No. 1.2 above). This also applies to the requirements issued by the Federal Constitutional Court regarding the handling of data from secret investigation measures by investigating authorities (see 26th Activity Report No. 1.3). The draft bill in its present form does not fully comply with these requirements. Firstly, the draft maintains the so far limited level of the division of tasks between the general customs administration and the customs investigation service. The assignment of tasks to the Customs Investigation Service is not limited to the prevention and prosecution of criminal and administrative offences, the detection of unknown offences and the preparation of future criminal proceedings within the competence of the customs administration. It also includes various support and participation tasks for the general customs authorities. The limits of the respective powers are not sufficiently clearly defined.

The Customs Criminal Investigation Office (ZKA, *Zollkriminalamt*), as the central institution, is also responsible for comprehensive risk management for all tasks performed by the customs administration, including customs investigations.

This task sets in at a very early stage and corresponds to low-threshold data processing powers, for example, already in the case of participation in the cross-border movement of goods. A differentiated regulation is lacking that distinguishes between the collection and the further use for the various fields of customs investigations and, if necessary, sets its own thresholds for this. Data that is processed in the context of risk management may not be processed automatically and without additional requirements also for the purposes of hazard prevention and preparations for law enforcement measures.

The lack of differentiation between the collection and the further use of data is omnipresent through the entire bill. This means that the principles established by the Federal Constitutional Court for limiting the purpose when data is further used cannot be adequately addressed. The JHA Directive does not stand in the way of further differentiation because it only sets a minimum standard and

always allows for higher national protection standards.

I consider the rules for stock data disclosure and allocation of IP addresses to be disproportionate. This is made possible whenever necessary for the tasks of the Customs Investigation Service. As a result, this information can be permanently retrieved and continuously added to existing data throughout the entire storage period.

I also consider the so-called 'unfounded-suspicion files' to be inadmissible. In these files, data on individuals is stored in precautionary files and processed further even though no negative prediction can be lawfully determined with regard to these individuals at the time of storage. Storage enables subsequent 'enrichment' of the data stock with the aim of being able to justify a negative prediction in the future. The data is stored here in order to create suspicion. Mere limitation of the storage period does not solve the problem.

The need for the new powers to use covert investigators is not sufficiently justified.

That being said, I expressly welcome the improvements that have already been achieved during the course of reconciliation of the draft law. For example, the draft included a provision for opening orders, the prediction requirements in the rules for telecommunications surveillance, for the collection of traffic and user data and for the identification and localisation of mobile phone cards and telecommunications devices were concretised and the initially foreseen drag-along mechanism for periods after which the elimination of data had to be examined was deleted again.

9.1.5 Control-free spaces in the area of intelligence services and co-operation with other supervisory authorities

There are unfortunately still areas where I cannot fully supervise the processing of personal data. I am trying to compensate for this by working closely with other supervisory bodies, as is also required by the Federal Constitutional Court.

The Federal Constitutional Court obliges supervisory authorities to co-operate via the intelligence services – an aspect designed to balance weak legal protection of individuals' rights against corresponding covert measures. However, the performance of this duty constantly means with new challenges.

Co-operation with the committees of the German Bundestag and the requirements of the Federal Constitutional Court for co-operation between the supervisory bodies were already described in my last activity report (see 26th Activity Report No. 10.2.10.2 and No. 10.3.5). During the current reporting period, I also co-operated extensively with the G10 Commission. Several joint successful inspections and fact-finding visits were carried out, the content of which I cannot elaborate on here for reasons of confidentiality.

Contacts also exist with the newly appointed Plenipotentiary of the Parliamentary Control Body. I would like to develop co-operation with the Parliamentary Control Body itself and also establish contact in the future with the Independent Body of the Federal Intelligence Service set up at the Federal Supreme Court with the task of supervising foreign telecommunications intelligence of the Federal Intelligence Service.

Control-free spaces can be due to different reasons. Either there are several control bodies whose responsibilities are not clearly defined or which, at least in practice, do not (or cannot) co-operate in such a way that data processing operations can be fully checked, or the legislator does not provide for comprehensive data protection control for certain areas from the outset.

The processing of personal data by the Federal Intelligence Services is controlled both by myself and by the G10 Commission which, however, controls data processing exclusively within the framework of restrictions against the secrecy of letters, post or telecommunications under the Act on Restricting the Secrecy of Letters, Post or Telecommuni-

cations (G10 Act, *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*), so that its material control competence is limited. This concerns requests by intelligence services to survey the telecommunications of individuals for whom the legal requirements pursuant to sec. 3 of the G10 Act are met. With regard to the distinction between my sphere of competence and that of the G10 Commission, I already commented on this in detail in the 24th Activity Report (No. 7.7.2) and since then have called on the legislator to clarify this (24th Activity Report No. 7.7.2 and 26th Activity Report No. 10.2.10.3). Such clarification is still lacking at legislative level. However, the legislator has introduced an at least rudimentary clarification in the reasons for sec. 26a of the Federal Constitutional Protection Act (BVerfSchG, *Bundesverfassungsschutzgesetz*) (added by art. 2 of the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680' (DSAnpUG-EU, *Datenschutz-Anpassungs- und Umsetzungsgesetz EU*) of 30 June 2017 – see No. 1.1). Since the coming into effect of this law, I carried out two joint inspections with the G10 Commission (see also No. 9.3.5). There were no problems in this respect during the inspection at the Domestic Intelligence Service (BfV, *Bundesamt für Verfassungsschutz*). During the inspection at the Federal Intelligence Service (BND, *Bundesnachrichtendienst*), the G10 Commission was not granted comprehensive access to all data on the grounds that the data in question was not "G10 data". I am talking to the Federal Intelligence Service, the Federal Chancellery and the G10 Commission about how joint constitutional control can be ensured in these cases. This problem is also the subject of a constitutional complaint (see also No. 9.1.6).

I have come across the phenomenon of control-free spaces due to a lack of legislative norms in the field of international cooperation between intelligence services. In 2016, the Federal Intelligence Service and the Domestic Intelligence Service were given legal power to participate in joint files with foreign intelligence services and to keep such files themselves under their own responsibility. As already stated in the 26th Activity Report, the Federal Ministry of the Interior, Building and Community and the Federal Chancellery deny me the authority to inspect on site the data of German intelligence services in files kept by a foreign intelligence service (see 26th Activity Report No. 10.2.10.1). They justify this by reference to the wording of the corresponding regulations in the Federal Constitutional Protection Act as well as in the Federal Intelligence Service Act, (BNDG, *Gesetz über den Bundesnachrichtendienst*) pursuant to which the rules concerning independent data protection supervision by the Federal Commissioner for Data Protection and Freedom of Information in cases of the establishment of joint files with foreign intelligence services apply only to data entered by the respective intelligence service and its retrievals. With regard to the sharing of files with foreign intelligence services, there is no reference to the rules on independent data protection control. Unfortunately, nothing has happened here since my last Activity Report.

I therefore recommend that the legislator create clear responsibility roles for the Federal Commissioner for Data Protection and Freedom of Information and the G10 Commission and also set forth rules for cooperation between these supervisory authorities. Furthermore, the control authority of the Federal Commissioner for Data Protection and Freedom of Information should also be comprehensively recognised and, if necessary, clarified when joint files are kept by the Domestic Intelligence Service and foreign intelligence services.

I recommend that the legislator create clear responsibility rules for the control activities of the Federal Commissioner for Data Protection and Freedom of Information and the G10 Commission, which also cover issues of cooperation between these two supervisory authorities. I also recommend that the control authority of the Federal Commissioner for Data Protection and Freedom of Information should be comprehensively recognised when joint files are kept by the Domes-

tic Intelligence Service and foreign intelligence services, and that clarifying legislation be adopted if necessary.

9.1.6 Current constitutional complaints in the field of intelligence services

During the reporting period, I commented on two constitutional complaints concerning the Federal Intelligence Service. The decisions are eagerly awaited. In one other case, I participated in the ongoing procedure by answering a questionnaire.

Statement on the constitutional complaint against the G10 Act and the Federal Data Protection Act

A constitutional complaint is currently pending before the Federal Constitutional Court which also deals with the relationship between the G10 Commission and the Federal Commissioner for Data Protection and Freedom of Information with regard to their control activities. Sec. 26a of the Federal Constitutional Protection Act (BVerfSchG, *Bundesverfassungsschutzgesetz*) which by reference also applies both to the Domestic Intelligence Service (BfV, *Bundesamt für Verfassungsschutz*), the Military Counter Intelligence Agency (MAD, *Militärischer Abschirmdienst*) and the Federal Intelligence Service (BND, *Bundesnachrichtendienst*) as well as sec. 15 (5) 2nd sentence of the G10 Act are claimed to be unconstitutional since the splitting up of the control task does not guarantee proper supervisory control of strategic telecommunications surveillance. The G10 Commission decides on the admissibility and necessity of restrictions on the secrecy of letters, post or telecommunications. Its power of control extends to the entire processing of personal data obtained under this act by the federal intelligence services, including the decision on communications to data subjects. Pursuant to sec. 26a of the Federal Constitutional Protection Act in conjunction with sec. 32 of the Federal Intelligence Service Act, (BNDG, *Gesetz über den Bundesnachrichtendienst*), I supervise compliance with data protection regulations by the Federal Intelligence Service. In as far as compliance with regulations is subject to control by the G10 Commission, it is not subject to my control unless the G10 Commission requests me to monitor compliance with data protection regulations in specific activities or areas and to report solely to it on this matter.

I have commented on this constitutional complaint and stated that I have long wished to see clearer legislation. This specifically applies to how the obligation to co-operate is designed and the clear distinction between spheres of responsibility. If the duty of supervisory bodies to co-operate is taken seriously by both the authorities supervised and their supervisors, it may be possible to interpret the rules in compliance with the constitution. It remains to be seen which view the court will adopt.

Statement on the constitutional complaint against the Federal Intelligence Service Act, (BNDG, *Gesetz über den Bundesnachrichtendienst*) in the version of the Act on Foreign Telecommunications Intelligence (BNDAAFAufklG, *Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*) of 23 December 2016

The action against the act that came into effect in January 2017 was brought by Reporters sans frontières and a number of journalists based in Germany and in other European and non-European countries. The subject of the constitutional complaint is the question of the constitutional conformity of the rules adopted for strategic foreign-to-foreign telecommunications intelligence with regard to the territorial and personal validity of the protection of fundamental rights as well as co-operation of the Federal Intelligence Service with foreign institutions.

The strategic foreign-to-foreign telecommunications intelligence is characterised by a broad-based approach aimed at obtaining data from communication networks in order to fulfil the legal mandate of the Federal Intelligence Service. For the purposes of this mandate, personal data from the networks

to be surveyed may be collected and analysed using so-called selectors. To put it simply, selectors can be referred to as search terms, such as telephone number ranges or domain names.

In the case of foreign-to-foreign telecommunications intelligence and depending on the given constellation, this can be communication data of foreigners recorded from within Germany or abroad. The law does not require a concrete reason to collect personal data of foreigners from abroad. The principle of strategic telecommunications intelligence thus stands in contrast to the principle of individual intelligence, which always requires concrete suspicion and judicial authorisation with regard to the individual concerned and hence prevents the state from blanket recording of personal data without cause. The principle of individual intelligence applies unrestrictedly in Germany.

The fact that no concrete reason is required for strategic foreign-to-foreign telecommunications intelligence means that the special protection which a participant in communications enjoys in Germany in relation to the German state, in particular also as a member of a group of persons who are holders of secrets for professional reasons (lawyers, physicians, journalists) and whose communications with clients, patients, eyewitnesses requires particular protection, is not granted. This reduced protection compared to the legal situation in Germany also applies, for instance, to the transmission of data to foreign intelligence services. The transfer of personal data within such co-operation schemes is partially automated.

The journalists who filed the action claim that the requirements for co-operation with foreign intelligence services mean that sensitive information about communications with journalistic sources is passed on without any further differentiation. Depending on which data is passed on in which co-operation relationship, this would lead to serious risks to journalists and their sources. Free journalistic activity is hence also significantly restricted.

I have commented on these facts from the point of view of data protection law against the background of case law of the Federal Constitutional Court and the current debate on the actual possibilities of the differentiated collection of telecommunications data. One key aspect of the statement addresses the fact that the Federal Constitutional Court, in view of the necessarily covert encroachments on fundamental rights by the Federal Intelligence Service, assigned the supervisory bodies a compensatory function (Federal Constitutional Court BVerfG 1 BvR 1215/07, para. 207, 1 BvR 966/09, para 14) for the protection of the fundamental rights of those affected. The implementation of this case law is the joint responsibility of the authorities and the legislator. However, this requirement has not yet been comprehensively met in the field of intelligence services. A further focus concerns the presentation of the growing importance of the right to informational self-determination in the field of intelligence activities in relation to other relevant liberties in light of the diversity of data collected by foreign-to-foreign telecommunications intelligence. Finally, I presented my practical assessment of the co-operation requirements for the supervisory bodies responsible for supervision of the Federal Intelligence Service. It seems necessary to provide a permanent basis for co-operation already underway so that comprehensive and effective control of intelligence services by the control bodies can be guaranteed as demanded by the Federal Constitutional Court.

Statement on the constitutional complaint against sec. 6a of Anti-terror File Act (ATDG, *Antiterrordateigesetz*)

In the context of a constitutional complaint against sec. 6a of the Anti-terror File Act, the Federal Constitutional Court gave me the opportunity to submit my comments and sent me a list of questions regarding facts relevant to the proceedings. Sec. 6a of the Anti-terror File Act regulates the extended project-related use of data stored in the anti-terror file. As a precondition for this, it must

be necessary to establish further facts of specific cases within the scope of a given case-related project for the collection and evaluation of information on international terrorist plans, where certain facts justify the assumption that offences of international terrorism as contemplated in in accordance with sec. 129a, 129b and 211 of the Criminal Code (StGB, *Strafgesetzbuch*) will be committed and that this constitutes a threat to the life, limb or liberty of individuals.

The provision was added to the Criminal Code when the Anti-terror File Act was amended in 2014, arguing that even complex queries of the anti-terror database were necessary. To my knowledge, the regulation has not yet been implemented in practice due to a lack of technical parameters, so that such use has not yet taken place. Irrespective of constitutional concerns, this fact alone should be reason enough to abolish the provision since it has proven to be superfluous.

9.2.1 Census 2021 in sight

Since the 2021 Census Preparation Act (ZensVorbG 2021, *Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2021*) came into effect in March 2017, preparations for the next census in 2021 have been underway. This year, I was extensively involved in work on amending this act with a provision for a trial run of the census and in the work on the 2021 Census Act.

The new sec. 9a that was added to the 2021 Census Preparation Act regulates the transfer by the respective statistical offices of the Länder to the Federal Statistical Office of certain data of all persons registered by German registration authorities as per the specified deadline. The aim is to review and further develop the transmission channels and the quality of the data records transmitted as well as the programmes for implementing the 2021 census. Sec. 9a (6) of the 2021 Census Preparation Act provides for the erasure of all data records processed for this purpose at the latest after completion of the trial phase which is scheduled for a maximum of two years.

I criticised the fact that the trial run will be carried out on the basis of real data from the registration authorities and that this data is to be kept available for the entire period of the trials. My request to carry out the trial run – at least temporarily – using pseudonymised data records and to provide for their successive erasure at the end of the respective parts of the trials was not taken up by the legislator. However, at my instigation, the explanatory memorandum at least clearly states that the preparations for the 2021 Census according to the 2021 Census Preparation Act and hence expressly also the trial run pursuant to sec. 9a of the 2021 Census Preparation Act are already part of the 2021 Federal Statistics Census and that in this respect the requirements of the Federal Statistics Act (BStaG, *Gesetz über die Statistik für Bundeszwecke*), such as secrecy pursuant to sec. 16 of the Federal Statistics Act and electronic data transmission pursuant to sec. 11a of the Federal Statistics Act, are applied. Since my concerns could not be completely dispelled in the legislative process, I will closely accompany the trial run for the 2021 census as the data protection supervisory authority responsible for the Federal Statistical Office.

Shortly before the end of the reporting period, I received the Draft Law on the Implementation of the Census in 2021 (ZensG 2021, *Entwurf eines Gesetzes zur Durchführung des Zensus im Jahr 2021*) as part of the interdepartmental coordination procedure. Just like the last census in 2011, this census too will be register-based and include a population as well as a building and housing census, a household survey on a sample basis and surveys at addresses with special areas.

9.2.2 Citizen portals and digital administration

With the Act to Improve Online Access to Administrative Services (Online Access Act (OZG, *Onlinezugangsgesetz*)), the Federal Government has created the prerequisites for interconnecting the administration portals of

the Federal Government, of the Länder and of municipalities. Citizens should have access to all administrative services offered online at an administrative portal of their choice without having to identify themselves more than once. The associated promise that further information will only have to be entered once must be implemented in such a way that it does not pose any risks to the privacy of data subjects.

If access to all administrative services offered electronically is to be provided from a single point of contact, this requires users to register for electronic access to administrative services via just one portal in order to then be able to use administrative services throughout Germany. The individual administrative services will continue to be offered by the respective competent authorities under their own data protection responsibility. Portal operators only have the right to transfer the data necessary for identification to the authority providing a particular administrative service. With this regulation, I welcome the fact that there are no plans to create a central database to serve all administrative services, that identification at a portal does not require the identity card to be used and that administrative services can also be used online without setting up a permanent service account. The 'core data record' that is sometimes discussed in conjunction with citizen portals is limited by the Online Access Act to the data required for identification.

During the reporting period, the concept of a sector-specific personal identifier was also pursued, which ultimately represents a leaner variant of a sector-spanning personal identification number with lifelong validity. The personal identification number is designed to ensure unambiguous classification and reliable retrievability. However, this also makes it considerably easier or even possible to merge the data stocks of individual authorities for purposes which may be considered to be comprehensible when viewed individually. This real use possibility, however, increases the risk of abuse. The resultant potential threat to the right to informational self-determination led the Federal Constitutional Court in 1983 to classify the creation of a system of personal identifiers as unconstitutional. This legal framework, which was developed by the supreme court, is still valid today and is the yardstick for the constitutional evaluation of any kind of personal identifiers.

This threat to the right to informational self-determination that arises from the possibility to compile catalogues can only be countered by creating some kind of 'equality of arms'. When it comes to implementing the Online Access Act, it is therefore important to ensure that citizens have full transparency at all times and can see which data they are providing to whom and for what purpose. It is essential that data subjects first consent to the automated collection of data from other sources if, for example, an application is processed using data which the data subjects would otherwise have to provide themselves. Details of the residential address for issuing a residential parking permit, for instance, may only be verified with the applicant's consent by means of an automated query in the residents' registration register. In the upcoming implementation of the Online Access Act at federal level with the establishment of a federal portal, I will ensure that these rules are observed.

9.2.3 A new legal basis for Europol

Europol has been given a new legal basis which also includes a new data protection supervision function and hence also a new role for me. Europol's mission is to support co-operation between EU Member States in order to prevent and combat organised crime, terrorism and other forms of serious crime involving at least two Member States. This is to be achieved especially by promoting the exchange of information between the EU Member States and the analysis of criminal investigation intelligence.

The legal framework for the performance of these tasks has changed considerably over the past 20 years, most recently as a result of a new Regulation which came into effect on 1 May 2017 (Regulation (EU) 2016/794 of

11 May 2016).

The new Regulation also implies a change in Europol's data protection supervision role. While the Joint Supervisory Body (JSB), made up of representatives of the data protection authorities of the EU Member States, was previously responsible for this task, it is now the European Data Protection Supervisor (EDPS) who has both more resources and more powers to carry out these tasks.

The new supervisory structure also changes my tasks. In addition to supervising the national central office, i.e. the Federal Criminal Police Office in Germany, I am now a member the newly established 'Advisory Board for Co-operation' together with the other national supervisory authorities and the EDPS. This Board is responsible for both general questions regarding the interpretation of the Europol Regulation and specific cases raised by national supervisory authorities or the EDPS. My authority appoints the deputy chair of the Advisory Board.

9.2.4 Machine Learning needs to be learned

Police and intelligence services also want to make use of state-of-the-art electronic data processing. Machine Learning is therefore finding its way into their IT landscapes in many ways and poses new challenges for all stakeholders. This does not necessarily call for a major revolution in the IT systems that drive and expand the possibilities to analyse existing data. In some cases, it is only technical progress, for instance, from video surveillance using conventional surveillance equipment to 'smart' video analytics using Machine Learning (ML). In contrast to 'hard-wired' programming, Machine Learning refers to procedures where the internal data processing model is trained during the development phase on the basis of selected and known data records.

The sensible use of ML techniques in the security sector requires large amounts of data to be available. In order to guarantee effective data protection supervision in these applications, the transparency of the individual processing steps is essential as is the evaluation of the effect and hence of the proportionality of fundamental rights encroachments within the framework of data processing by the authorised authorities. The effect of current ML methods is by definition essentially determined by the quality and systematics of the training data used during the development of the respective software product.

The use of training data for development purposes, in particular, poses a data protection problem: The training of ML models with real data can, depending on its content, already constitute processing of personal data. Furthermore and depending on the method used, a review of the training phase, which may have been completed long ago, may be necessary during subsequent live operation in order to understand and assess the IT system. At an early stage of the respective project, it must be decided how the documentation, development processes and mode of operation of the individual systems are to be designed in order to comply with data protection law and to enable the required effective data protection supervision.

To date, none of the authorities working in this field have informed or involved me regarding the processing of personal data within the framework of the development of new IT systems for the purpose of training ML models. In future, however, the source of the training data for such technical systems will have to be scrutinised by data protection authorities. At several consultation and fact-finding meetings during the reporting period, this issue was already addressed in different contexts. During trials in the context of developments and product approvals of IT systems, the use of real data is subject to strict requirements due to its restrictive purpose limitation. I repeatedly pointed out at meetings that the same procedures must also apply to the training of ML models. One possible way would be to use synthetic data, which for many reasons is the best choice for developing and testing conventional and ML-based IT. This technologically demanding

task would indeed permanently help to avoid problems with the introduction of future ML-based IT processes from the very outset.

9.2.5 Effective data protection according to the 'state of the art'

The aim of the GDPR is to achieve optimum protection of the rights of data subjects. An important building block for this is technology design that complies with data protection and data security. Besides other requirements, the GDPR demands that the 'state of the art' be taken into account. How is this 'state of the art' defined? Reference to the 'state of the art' can be found in several places in the GDPR, for example, in conjunction with the central obligation to ensure data security in art. 32 of the GDPR. Controllers and processors within the meaning of the GDPR must implement appropriate technical and organisational measures in order to ensure protection against unauthorised access, unlawful processing or unintentional loss of data. However, the state of the art must also be taken into account pursuant to art. 25 (1) GDPR which addresses the issue of data protection by design and default. Recitals 78 and 83 also refer to the state of the art: Producers of products, services and applications are to be encouraged to adequately take into account the right to data protection and the state of the art. Measures, such as encryption, must ensure a level of protection appropriate to the risks posed by the processing and the nature of the personal data to be protected, taking into account the state of the art and the costs of implementation.

In all these cases, the 'state of the art' clause is intended to ensure that the best technology available in practice is used. This refers to success models that are based on proven findings and are sufficiently available in order to be adequately implemented. Relevant international, European and national norms and standards are to be taken into account in particular, but also other concepts that have already been tested in practice. The obligation therefore does not preclude the possibility of new or different concepts if this ensures equally effective protection.

National and European data protection supervisory authorities need to work together in order to clarify which technical and organisational measures correspond to the state of the art and to ensure uniform requirements for private business and public administrations. This is the only way to ensure a uniform European level of data protection for products, services and applications that are generally available worldwide.

9.2.3 Projects of the Federal Police

During the period under review, the Federal Police launched two projects that are controversial under data protection law, i.e. testing facial recognition software at Südkreuz railway station in Berlin and testing bodycams. I became involved too late and not to a sufficient extent. In August 2017, the Federal Police launched the pilot project at Südkreuz railway station, initially with the testing of facial recognition software. Three different software products for facial recognition were used in the live operations and their suitability for use in practical police work was tested. Footage from selected cameras of the video-surveyed railway station was compared with a mock stock of wanted persons' photographs that was created from photographs taken by voluntary test subjects. Processing was carried out in a separate and isolated network and reconciliation with police databases did not take place. The test subject recognition rate was evaluated.

Although I was informed about the project in the run-up to trial operations, communications did not remain that good in the long run. For example, I first learned about the use of active transponders from the press and could only respond to this instead of being proactively involved beforehand. I

also did not receive the final report of the first test phase as usual, i.e. before its publication, even though I had requested it several times. The second test phase is currently being planned, during which several scenarios will be tested, such as entering defined areas and recognising people lying down. The plans for this were communicated to me in several information events so far.

Although I understand that video surveillance with face recognition can be a good tool in everyday police work, I consider the use of this new technology, which goes beyond conventional video surveillance, in everyday police work to be unlawful in the current legal environment. Face recognition is an intervention-intensive measure that affects a large number of people. This intervention requires a sufficiently determinate legal basis which presently does not exist. It is questionable whether the high constitutional requirements for correspondingly far-reaching encroachments on fundamental rights can be met at all.

The test and the planned introduction of bodycams is another important project by the Federal Police. Bodycams are portable video recorders that officers can attach to their clothing and activate and deactivate as required.

They are intended to help offers protect themselves better and to improve documentation of conflict situations. Recordings may only be made in the public space and after prior announcement. In the first tests, the Federal Police found a significant de-escalating effect. The legal basis for use is sec. 27a of the Federal Police Act (see No. 9.1.3 above). I am currently discussing with the Federal Police the question as to where the video data is to be processed and stored. The Federal Police and my authority have conflicting views on this matter. After information regarding the planned storage type was provided only at a very late point in time in this case too, i.e. without prior reference and only at the time of submission of the changed draft of the opening order for the bodycam, I hope that I will be informed sooner in future.

9.3.4 Projects of the Federal Criminal Police Office

With the 'Police 2020' programme, the IT landscape of the German police is set ot undergo fundamental reorientation. This also shows that the Federal Criminal Police Office is increasingly positioning itself as a central IT service provider for the police, such as the uniform case management system and a new telecommunications surveillance system. The previous compound files of the nationwide police information system (INPOL) are to be abolished and replaced by a new information network as part of the 'Police 2020' programme. The basis for this is the amended Federal Criminal Police Act (see No. 9.1.3). I already submitted extensive critical comments on the draft law (see 26th Activity Report No. 10.2.9.1).

Unlike in the past, the police data network is no longer to be divided into different logically separated files. Instead, the Federal Ministry of the Interior, Building and Community and the Federal Criminal Police Office intend to create a 'joint data house'. Police data will then be kept in this house for the police forces of the Federation and the Länder. However, rules for access to this data have not yet been sufficiently clarified. In particular, the criteria according to which access rights for individual users will be assigned have yet to be defined. It goes without saying that other fundamental issues of data protection law must be considered in this context. First of all, however, it should be noted that neither the Federal Ministry of the Interior, Building and Community nor the Federal Criminal Police Office have provided me with detailed and meaningful documents for the planned

new IT structure of the German police. Only some details are known to me. The basis for a detailed assessment under data protection law is hence still lacking.

'Police 2020' is a programme designed to take several years. It is still unclear when the new IT landscape will be introduced. However, the files which currently exist will be retained at the same time under transitional rules. From today's perspective, this project is highly unlikely to be introduced in 2020 despite its ambitious name.

The new information network will also integrate existing projects and procedures, such as the provision and operation of a uniform case management system by the Federal Criminal Police Office. The uniform case management system is still in the process of being set up. The aim is to consolidate the decentralised case management systems of the police forces into a uniform management system.

Independent of the 'Police 2020' programme, the Federal Criminal Police Office submitted to me its PHOENIX project to implement a next-generation telecommunication surveillance system.

The aim of the project is to set up a next-generation telecommunication surveillance system as a central service offering for joint use by different authorities. The project is still in its initial phase. Specifications are currently being drawn up. Since telecommunications surveillance typically involves a major data protection component, I will accompany the project under data protection law.

The problems that may arise in the new information network are also illustrated by experience gained from inspections which I carried out in the past, for example, regarding the processing of identification data or on the narcotics case file.

I already reported several times in the past on the processing of identification documents (21st Activity Report No. 5.2.4.1; 22nd Activity Report No. 16.21; 24th Activity Report No. 7.4.3). I recently pointed out that a separate deadline for the examination of the need to erase incorrect or unlawfully transmitted data must be allocated to identification data, so that this data is separated more strictly from other personal data and can be erased separately. Furthermore, the Federal Criminal Police Office was obliged to ensure that it only stores identification data based on its own findings. In the meantime, both responsibilities and erasure rules were revised. The system of shared responsibility, which I criticised, will no longer be used. During the course of this change process, comprehensive data cleansing was initiated and is still ongoing in the area of identification data. Up to now, around 2.1 million files and/or entries have already been deleted, and hundreds of thousands of new files were created according to the new rules and provided with dedicated deadlines for the examination of the need to erase incorrect or unlawfully transmitted data. The process is expected to continue until 2023.

The control of the narcotics case file was also very successful (26th Activity Report No. 10.3.2). On a positive note, I found a significant reduction in the number of cases stored since then. In the area of customs investigations alone, of the 54,543 individuals originally stored (as of 30 June 2015) only 11,091 are still stored in the new interconnected system after the cleansing process associated with the migration to a new file. This means that 43,452 personal data records stored unnecessarily were deleted at federal level alone. There were also significant, albeit very different, reductions in the volumes of data stored at Länder level.

9.3.5 Mandatory inspections in the

field of internal security

Both national laws and EU law increasingly provide for data protection inspections for certain files or investigative measures to be carried out on a regular basis. First experience with the different mandatory inspections was already gained.

National mandatory inspection of 'unloved files'

National law obliges me to verify at least every two years whether the authorities that store data use the anti-terror file and the right-wing extremism file in compliance with data protection law.

Whilst these inspections have become well established, the two files tend to be the 'stepchildren' of the authorities concerned. The question hence arises as to whether they still make sense.

During the current reporting period, I carried out the following inspections:

Anti-terror file: Federal Police (BPol) (2017), Customs Criminal Investigation Office (ZKA) (2017), Domestic Intelligence Service (BfV) (2017), Military Counter Intelligence Agency (MAD) (2018), Federal Intelligence Service (BND) (2018). Right-wing extremism file: Federal Criminal Police Office (BKA) (2018), Federal Police (BPol) (2017), Domestic Intelligence Service (BfV) (2017), Military Counter Intelligence Agency (MAD) (2017). I will probably not have to issue a complaint as a result of any of these inspections; some inspections were not yet completed by the copy deadline.

I found that the police authorities handled the data in a way that was commensurate with the sensitive nature of the files. The storage requirements were thoroughly checked and were usually easy to understand. The systems are subject to strict security measures and strict authorisation concepts. So far I only had to issue minor recommendations regarding the handling of the files.

The inspections of the anti-terror file at the Domestic Intelligence Service and the Federal Intelligence Service were carried out as joint inspections with the G10 Commission of the German Bundestag (see No. 9.1.5).

During the inspection of the anti-terror file at the Military Counter Intelligence Agency, my staff were accompanied by a member of the secretariat of the G10 Commission. Although the Military Counter Intelligence Agency had stated in the run-up to the inspection that it did not store any 'G10 data' in the anti-terror file, so that participation of the G10 Commission was not considered to be necessary, the participants agreed that I would ask the G10 Commission to accompany me in order to be able to inspect, if necessary, any 'G10 data' which we did find during the inspection. This approach turned out to be practicable.

The Domestic Intelligence Service has meanwhile remedied the procedures and errors which I had criticised in the past (see 26th Activity Report No. 10.3.5). For example, responsible staff were trained and technical problems on the part of the storing authorities were eliminated or minimised.

However, I found during all these inspections that the authorities inspected consider the value of both files for counter-terrorism and anti-extremism purposes to be rather low. All in all, my impression was also that the purpose of the files, i.e. to create a contact initiation tool for the authorities involved, is not achieved either.

The design of both files is obviously not flexible enough for everyday police work. Information essential in the fight against terrorism and extremism is in practice exchanged at the common centres of the authorities, i.e. the Joint Centre for Countering Extremism and Ter-

rorism (GETZ, *Gemeinsames Extremismus- und Terrorismusabwehrzentrum*) and the Joint Counter-Terrorism Centre (GTAZ, *Gemeinsames Terrorismusabwehrzentrum*). The work of these centres was described to me as being more target-orientated than the operation of the right-wing extremism and anti-terror files. This also corresponds to the assessment by the intelligence services. In relation to the benefit, staff at the authorities have to invest an enormous amount of time and effort in order to enter, update and erase the relevant data in compliance with the law. In addition, the technical problems already mentioned in the previous Activity Reports still exist and make using the anti-terror and right-wing extremism files even more difficult (see 26th Activity Report No. 10.2.10.1 and No. 10.3.5).

I therefore began to discuss this topic with the Federal Criminal Police Office as the authority storing the files and the Federal Ministry of the Interior, Building and Community as its supreme supervisory instance (see No. 9.3.11).

Mandatory inspections regarding the use of European systems

EU law requires mandatory inspections to be carried out in three areas. These are the national use of the second-generation Schengen Information System (SIS II) and, in individual cases, searches by the security authorities in the Visa Information System (VIS) and in the European Eurodac database which are permitted in individual cases (see No. 2.2).

Such inspections were carried out for the first time during the current reporting period:

SIS II: Federal Criminal Police Office (BKA) (2017), Federal Police (BPol) (2018)

VIS queries: Federal Police (BPol) (2017), Customs Criminal Investigation Office (ZKA) (2018), Domestic Intelligence Service (BND) (2018)

Eurodac queries: Federal Criminal Police Office (BKA) (2017), Federal Police (BPol) (2018)

Since April 2013, the police and border control authorities of the Schengen area have been using SIS II for central alerts on persons for the purpose of refusing entry and stay pursuant to Regulation (EC) No 1987/2006 of 20 December 2006, and for central person and property searches for the purposes of police and judicial cooperation in criminal matters on the basis of Council Decision 2007/533/JHA of 12 June 2007 (see No. 1.3). I am obliged to verify use of the system in compliance with data protection on a regular basis and the security standards at least every four years.

During the period under review, I determined the security precautions existing at the Federal Criminal Police Office for the national components of the system as well as the extent of the logging of storage prerequisites and issued corresponding recommendations. This specifically concerned the necessary predictive decisions for preventive entries in search lists for the refusing stay and entry. On the other hand, no shortcomings were found in the field of police co-operation with regard to entries in search lists.

Since 2013, the police authorities and intelligence services are entitled under certain conditions to perform data queries in the Visa Information System. The inspections carried out did not give rise to any objections. In the cases examined, queries were carried out in a specific hazard prevention or investigation procedure in order to defend against or prosecute sufficiently serious criminal offences and also appeared to be suitable for promoting the objective of the query. There was nothing to complain

about at the Customs Criminal Investigation Office. Documentation there was complete and easy to understand. I issued a recommendation to the Federal Police to improve documentation because the need for queries was not always apparent directly from the content of the files. The inspection at the Domestic Intelligence Service was not yet completed by the copy deadline.

Since 2015, the police authorities have been authorised under certain conditions to check fingerprints against data of asylum seekers in Eurodac. Little use has so far been made of this possibility, probably due to restrictive access requirements as well as the relatively small amount of data (for example, no photographs). One additional condition for access – the remaining ones being designed analogous to the VIS – is the so-called query cascade which means that certain other databases have to be searched first within a reasonable period of time (and not, for instance, three years before the Eurodac query as in one of the cases examined). As a result, I recommended that the Federal Criminal Police improve its documentation. The inspection at the Federal Police was not yet completed by the copy deadline. However, documentation shortcomings are already apparent at this organisation too.

I recommend that the police authorities make sure they have meaningful documentation when accessing Eurodac and the VIS Information System. I recommend that the legislator abolish the anti-terror and right-wing extremism files in view of their limited practical value.

9.3.7 Accreditation procedure at the G20 summit

On 6 and 7 July 2017, 32 journalists who had initially been granted accreditation to cover the G20 summit in Hamburg, had their accreditation withdrawn. This subsequently led to the accusation of data protection violations in conjunction with the accreditation procedure and the storage of personal data in police and security authority files. This prompted me to examine both the accreditation procedure and the handling of the personal data of the journalists concerned. The accreditation procedure was carried out by the Federal Criminal Police Office. The decisions were based on personal data collected by the federal police authorities, the Domestic Intelligence Service and the police and domestic intelligence authorities of the Länder and/or fed into the nationwide information systems.

Most of the decision-relevant information concerned data stored under the responsibility of the Länder. My data protection supervision and evaluation activities had to be limited to data from the federal authorities because my colleagues at the Länder are responsible for the data of their respective Länder. As a result, I concluded that the accreditation procedure for the G20 summit, in as far as the Federal Criminal Police Office was responsible, was unobjectionable in terms of data protection law with regard to the 32 journalists whose cases were investigated. Although the Federal Criminal Police Office issued a list of names of journalists to officers of the Länder police without being entitled to do so, the Federal Criminal Police Office argued that this happened unintentionally. Since this was not a structural shortcoming, but a mere oversight and because the Federal Criminal Police Office itself had detected this mistake and promised to avoid it in future cases, I did not raise any objections in this respect either.

The Domestic Intelligence Service had, under its own data protection responsibility, stored data on 14 individuals whose accreditation had been withdrawn and had transmitted this information to the Federal Criminal Police Office. Both the storage of the data and its transmission were lawfully carried out with regard to 13 of these individuals. In one case, it was not possible to assess whether

the transmission was lawful because the authorities had unlawfully failed to handle the case on its individual merits. The Domestic Intelligence Service already informed me during the inspection that it had come to the conclusion that the data record was no longer necessary for the performance of the task and could be erased. However, it could not be erased until my inspection was completed. After I had declared the inspection to be completed, the Domestic Intelligence Service informed me that the data record had then been deleted.

Since I saw a need to check the quality of police and intelligence data even beyond my area of responsibility, I informed the respective data protection commissioners of the Länder with regard to the data storage by the Länder authorities discovered during my inspection and left it to the Länder authorities' discretion to perform inspections under their own responsibility.

A final report on this topic to the Interior Committee of the Bundestag, which also takes into account the test results of the Länder intelligence services involved, is currently being coordinated with these authorities.

9.3.8 Transmission of passenger data to customs authorities

I received notification that shipping companies transmitted passenger lists to customs authorities. After my examination and conclusion that the measure was unlawful, this practice was immediately discontinued. This contributed significantly to greater data protection in the area of customs.

The shipping companies of the German Baltic Sea ports were requested by customs investigation offices to forward all passenger lists to customs without any restrictions. I took this as an opportunity for an inspection. I found that all passenger lists of shipping companies operating ferry lines between the Baltic ports and Scandinavia were requested by customs. The passenger lists of cruise ships operating in the area were also affected. The customs authorities suspected this area to be a regular route for cigarettes and drug trafficking and attempted to use this measure as a means for successful investigation. The customs authorities referred to sec. 208 (1) (3) and sec. 93 of the Fiscal Code of Germany (AO, *Abgabenordnung*), the general clause in sec. 24 (1) and sec. 27 (1) of the Customs Investigation Act (ZFdG, *Gesetz über das Zollkriminalamt und die Zollfahndungsämter*) and, alternatively, the voluntary nature of the shipping companies' data transfers.

My examination revealed that there was no legal basis for this significant encroachment on fundamental rights. The Fiscal Code of Germany did not constitute a legal basis since there was no sufficient cause for investigation. The general clause of the Customs Investigation Act is not sufficient for such far-reaching intervention which affects an indefinite number of innocent citizens. Nor was it possible to claim the voluntary contribution by the shipping companies with regard to transfers since such extremely intensive intervention always requires a sufficiently determinate legal basis. I was able to convince the customs administration of this view. The transmission of passenger lists was stopped immediately and no objections were raised.

9.3.11 Anti-terror file and the right-wing extremism file – signs of fatigue

The anti-terror file, just like the right-wing extremism file, was created with great hopes of improving co-operation between security authorities. Both files fail to meet this claim and to fulfil the hope placed in them.

Data protection controls relating to the anti-terror and right-wing extremism files are very complex: Besides the storage in the files themselves, the so-called source files of the authorities storing the data must be examined. It is also difficult to check the storage on the basis of log data. First talks

were held with the Federal Ministry of the Interior, Building and Community and the Federal Criminal Police Office in order to improve this unsatisfactory situation.

During the inspections, the mood of the users was clear: The participating authorities have long since lost their interest in both files. The possibility of analysing these files pursuant to sec. 7 of the Right-wing Extremism File Act (RED-G, *Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus*) and sec. 6a of the Anti-terror File Act (ATDG, *Antiterrordateigesetz*) has not yet been realised (see also No. 9.1.6) and appears not to have been demanded by the security authorities to be absolutely necessary. Based on the impressions I gained from practical inspections, consideration should be given to abolishing these files due to their minor significance (see also No. 9.3.5).

11 Committee on Legal Affairs and Consumer Protection

11.1 From the legislative projects

11.1.1 Law to Strengthen Fair Competition

Final court decisions regarding the relationship between competition law and the GDPR must put an end to the uncertainties that still exist. I consider a legal restriction of the possibilities for an abusive use of cease and desist requests to be a meaningful parallel measure.

The coming into effect of the GDPR on 25 May 2018 led to fears, especially among small and medium-sized enterprises, of mass and abusive requests to cease and desist due to alleged violations of the GDPR. Although the feared wave of cease and desist requests did not materialise, uncertainty still exists. The question as to whether cease and desist requests under competition law with regard to violations of the GDPR are permissible under the Act Against Unfair Competition (UWG, *Gesetz gegen den Unlauteren Wettbewerb*) is controversial in literature and has not yet been conclusively clarified by case law.

In the meantime, the Federal Ministry of Justice and Consumer Protection has included a provision in its draft bill to strengthen fair competition which excludes the right to reimbursement of the costs of cease and desist requests from competitors in the event of violations of all information and labelling obligations on the Internet. This at least prevents any incentive for abusive cease and desist requests in the case of violations of the provisions of the GDPR on data protection policy statements on the Internet.

In view of this unclear legal situation, it will probably be left to the European Court of Justice to make a final decision on the relationship between competition law and the GDPR.

11.1.4 Proposal for an e-evidence Regulation

New possibilities for production orders are intended to fundamentally change the cross-border collection of evidence. With its draft e-evidence Regulation, the European Commission made a corresponding proposal to this effect. I reject this draft in its current version, because it currently fails to generally foresee the involvement of the judicial authorities at the provider's place of business, so that a major procedural safeguard does not exist. If evidence in criminal proceedings is located abroad, the investigating law enforcement authority must request legal assistance there. Should this principle change in the digital age simply because 'electronic evidence' is now globally available regardless of the physical location of its storage or territorial boundaries?

The European Commission has submitted a proposal for a new Regulation authorising law enforcement authorities in the Member States of the European Union to require providers of telecommunications and Internet services in other EU Member States and in third countries to transmit inventory, traffic and content data in criminal proceedings. The warrants would be binding on all providers offering their services in the EU. If the company does not have its seat in the EU, it would have to appoint a representative to whom the production order would be served.

I understand the Commission's interest in a proposed procedure that speeds up criminal investigations. However, together with my colleagues in the Länder, I reject the draft as it stands. This position was adopted by the Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder in a resolution of 7 November 2018 (available at www.datenschutz.bund.de).

In a detailed opinion, the European Data Protection Board, with my participation, also raised a number of critical questions, some of which I would like to address in this report. The full text of the opinion is available at: www.datenschutz.bund.de

One major point of criticism concerns the bypassing of the judicial authorities of the state in which the provider requested to produce evidence has its seat. Requests to providers in Germany are only brought to the attention of the German judiciary if the undertaking refuses to transmit the data and is requested by the judicial authority of the requesting Member State to execute the order. It therefore depends solely on the conduct of the requested provider whether the legality of the request is verified outside the requesting state. I am in no way suggesting that providers lack legal knowledge or legal intuition. However, it is also true that they pursue their own economic interests and are subject to obligations other than those of judicial authorities.

Another problem is that the proposal no longer makes the disclosure of data dependent on whether the offence is at all punishable in the requested state. Cases are therefore conceivable where companies based in Germany are obliged to transmit data to other European investigating authorities for the prosecution of criminal offences even though the offences in question are not punishable in Germany, for example, in the case of political statements. Companies could object to such requests, but would be threatened with sanctions if they did not comply.

It is also to be feared that third countries will use the EU regulation as a blueprint for their own regulations. Providers in EU Member States would then find themselves increasingly exposed to surrender orders from third countries, which could be used to prosecute crimes based on a completely different legal tradition.

The draft is currently under discussion in the Council of the European Union and the European Parliament.

14 Committee for the Scrutiny of Elections, Immunity and the Rules of Procedure

14.1.1 Between data protection and the free mandate – The validity of the GDPR in the German Bundestag

The provisions of the GDPR also apply mutatis mutandis to the German Bundestag, the parliamentary groups and the members of parliament. However, data protection supervision does not take place.

When the GDPR came into effect on 25 May 2018, the question arose as to what extent the provisions of the GDPR apply to the German Bundestag, the parliamentary groups and committees and individual members of parliament and whether they are subject to my supervision under data protection law (see also No. 1.1 above). The aforementioned institutions and individuals process personal data for a variety of purposes. For example, data from citizens is processed in the context of petitions or enquiries (for instance, from constituencies). The same applies to public relations work, for example, via parliamentarians' homepages or the diverse activities of members of parliament in social networks. Last but not least, members of parliament are also employers and hence also process their employees' personal data. However, processing operations connected with legislative activity do not fall within the scope of European law. In this respect, the GDPR does not apply directly, but mutatis mutandis via sec. 1 (8) of the Federal Data Protection Act. This means that the GDPR must also be observed for these processing operations. Since the German Bundestag, the parliamentary groups and committees as well as individual members of parliament are public bodies of the Federation, I am objectively responsible for these (sec. 9 of the Fedetral Data Protection Act). However, I do not have any supervisory powers in the area of legislative activity, to which the GDPR belongs as a simple federal law. Constitutional requirements, especially the principle of the separation of powers (art. 20.2 2nd sentence of the Basic Law for the Federal Republic of Germany (GG, *Grundgesetz für die Bundesrepublik Deutschland*) and the free mandate (art 38.1 2nd sentence 2 GG), contradict this. Notwithstandinng this, I also perform my consulting tasks in this area.

For the future, I recommend that the German Bundestag give itself its own data protection rules based on the requirements of the GDPR. The data protection rules should also provide for an internal data protection supervisory body which could receive and process complaints from data subjects concerning the processing of their personal data. Corresponding rules exist, for instance, in Schleswig-Holstein.

In order to answer the most urgent questions of the members of parliament regarding the GDPR, I prepared a guidance document which was sent to the members of parliament in December 2018. This guidance document is also available on my website at: (https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-GVO/Aktuelles/Aktuelles_Artikel/BfDIBeraetAbgeordneteBT.html?cms_templateQueryString=Hanreichung&cms_sortOrder=score+desc).

15 Committee on Economic Affairs and Energy

15.1 From the legislative projects

15.1.1 Confusion about the further applicability of Part 7 of the Telecommunications Act

Whether the Telecommunications Act (TKG, *Telekommunikationsgesetz*) will be adapted to the GDPR is uncertain now that the Federal Government has withdrawn the corresponding draft law at short notice and without giving reasons. The GDPR has been in effect since 25 May 2018. As a directly applicable European regulation, it generally takes precedence over national data protection law unless national provisions must be given priority on the basis of a collision rule, an implementation mandate or an opening clause of the GDPR. The national data protection provisions of the Telecommunications Act are only applicable to the extent to which they serve to implement the e-privacy Directive (Directive 2002/58/EC) (see art. 95 GDPR). Since 25 May 2018, for instance, the processing of data stocks, i.e. customer data collected for the purpose of establishing, structuring the content of, amending or terminating a contract for telecommunications services (sec. 3 No. 3 of the Telecommunications Act), has been primarily subject to the provisions of the GDPR. However, details as to when the GDPR and when the Telecommunications Act are to be applied to a given situation are still unclear. This is due to the fact that the 7th part of the Telecommunications Act has not yet been adapted to the new legal situation and misleadingly still contains provisions that have no longer been applicable since 25 May 2018 due to the priority application of the GDPR. This leads to great legal uncertainty for companies and customers. Many affected stakeholders therefore contacted me during the reporting period and asked for support in legal matters. Besides many consultations with telecommunications companies and processing inquiries from citizens, I therefore repeatedly drew the legislator's attention directly to the mandatory, timely adjustment of the Telecommunications Act. The first ministerial draft bills for the Second Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680 (2. DSAnpUG-EU, *Zweites Datenschutz-Anpassungs - und Umsetzungsgesetz EU*) therefore still demanded the necessary adaptation of the Telecommunications Act. However, these plans were then discontinued at short notice and without giving reasons (see also No. 1.1). There is an urgent need for action here on the part of the legislator.

15.1.2 The long labour pains of the e-privacy Regulation

In the 26th Activity Report (No. 17.2.4.1), I already reported on the reform of the e-privacy Regulation and ended with the European Commission's draft that was presented on 11 January 2017. The e-privacy Regulation, which has been in the legislative process since then, is intended to regulate the handling of data and information within the framework of electronic communications and to concretise the GDPR in specific areas. Since developments in the electronic communications sector are progressing at a rapid pace, the Regulation is of paramount importance for the protection of privacy in this area. In this respect, the originally planned time schedule according to which the e-privacy Regulation was to enter into effect at the same time as the GDPR was definitely a sensible consideration in order to implement the necessary legal adjustments with the shortest possible delay following rapid technological innovations.

The Working Party on Telecommunications and Information Society of the European Council has been discussing the Commission draft since February 2017, but so far without a final result. In the meantime, the Council has submitted several drafts for further dis-

cussion. The latest drafts, in particular, show a gradual softening of the rules at the expense of data protection and a lack of balance between the legitimate interests of users and industry. This is particularly evident in the example of Article 6 where the catalogue of facts justifying permission to process electronic communication data is to be extended in many respects. I take a critical view, for example, of the proposals to introduce a provision similar to art. 6 (4) GDPR permitting the processing of data for purposes other than the original purpose of collection. Such a norm constitutes an unacceptable exception to the data protection law principle of purpose limitation and does not adequately reflect the sensitive nature of electronic communications data protected by the telecommunications secrecy of art. 10 of the Basic Law.

→ I repeatedly expressed my opposition to making user access to certain online services dependent on the user's consent under data protection law. Such cookie walls do not meet the requirements for voluntary consent. Otherwise, financially disadvantaged users would have to pay with their data or even forego certain offerings, such as information from online media. It is important to me that the purpose of Article 8, i.e. to give users control over their devices, is not bypassed.

I am committed to better enshrining the principles of privacy by design and privacy by default in the Regulation. I therefore support Article 10 of the draft adopted by the parliament, which states that privacy by design is to be implemented through data protection-friendly default settings when software is installed. In order to support and speed up negotiations, the Article 29 Working Party published a first assessment of the draft in April 2017 (Opinion 01/2017 – Working Paper 247 of the Article 29 Working Party). On 28 May 2018, the European Data Protection Board (EDPB) issued a further opinion on the current legislative procedure. The aim of the publication was to clarify specific issues raised by the proposed amendments by the legislative bodies. The EDPB demands, for instance, that the new regulation enforce the consent requirement for cookies and similar technologies and that service providers provide technical tools for obtaining consent. The Board also points out that the future regulation must not under any circumstances fall short of the current level of protection.

At national level, many departmental discussions have now taken place in which my position is unfortunately not shared by all sides. At a public meeting of the EU Member States in Brussels on 8 June 2018, the German representative demanded "that the use of online services financed by advertising can be made dependent on the user's consent to the setting of cookies for advertising purposes". This ignored my demand and that of the data protection commissioners of the Länder which we had already published on 5 February 2015 in the resolution entitled "No cookies without consent" (*Keine Coookies ohne Einwilligung*). The background for this German position may have been the stakeholder meetings with representatives of industry and NGOs. For example, the Federal Ministry for Economic Affairs and Energy commissioned its in-house WIK Institute to prepare an expert opinion on the effects of the Commission's draft on the Internet/advertising industry, in which only stakeholders from the digital economy, publishing houses and the online advertising industry were interviewed. In my press release of 1 December 2017 on this study, I made it clear that the potential opportunities that could arise for the industry as a result of the changes favoured by me were not even marginally considered, and made it very clear that data protection must not be driven by commercial considerations.

On a positive note, the Federal Government shares my position that the e-privacy Regulation should also apply after the communication has been received and after the transmission has ended. This point is a shortcoming of the Commission's draft, which seeks to protect data only during transmission.

In order to create a legal framework in the field of electronic communications corresponding to that of the GDPR, the e-privacy Regulation must be adopted as quickly as

possible. The current application of the national provisions adopted on the basis of Directive 2002/58/EC no longer adequately reflects current developments and creates legal uncertainty for all the parties concerned. Questions regarding the applicability of national law parallel to the GDPR arise time and again (see also No. 15.1.1 and No. 15.2.4).

Telemedia: Cookies and more

Before 25 May 2018, I received several requests for advice from both telecommunications service providers and public authorities of the Federation asking for clarification as to which rules will apply to the use of cookies in the future. I also received many questions from citizens regarding the extent to which the setting of cookies is still permitted under the GDPR. My colleagues in the Länder had a similar experience in this area. After the data protection supervisory authorities learnt in March 2018 that the Telemedia Act (TMG, *Telemediengesetz*) would not be part of the draft of a Second Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680, a sub-working group of the Conference on Data Protection (DSK, *Datenschutzkonferenz*), of which I am a member, directly addressed the legal situation in the area of telemedia, taking into account the GDPR and the TMG that had not been adapted. Our position regarding the Telemedia Act which, in sec. 11 to 15a, contains data protection provisions for the relationship between providers and users of telemedia was adopted by the Data Protection Conference on 26 April 2018 and subsequently published (available at www.datenschutz.bund.de).

As a result, the specific data protection provisions of the Telemedia Act can no longer be applied parallel to the GDPR. Especially since the provisions are not a transposition into national law of the e-privacy Directive, they will not impose additional obligations on the grounds of art. 95 GDPR. Whether the processing of personal data is also lawful in the field of telemedia is therefore now assessed on the basis of the GDPR.

In order to exchange views with the companies and associations concerned, the Data Protection Conference initiated a consultation procedure in the summer of 2018. 19 associations/companies made use of this possibility. In October 2018, individual stakeholders were invited to a meeting with several data protection supervisory authorities in order to discuss with them their views from the written consultation procedure. Comments on the position are now to be finalised by the sub-working group and the Data Protection Conference will make them available to the groups concerned. This is important because the e-privacy Regulation is still a long way off and the adaptation of the Telemedia Act cannot be expected in the near future. In order to protect the data of users, I will work to ensure that it is published quickly.

I strongly recommend that the e-privacy regulation be adopted as soon as possible. The current application of the national provisions adopted on the basis of Directive 2002/58/EC no longer adequately reflects current developments and creates legal uncertainty for all the parties concerned. This specifically applies to the relationship between the German Telecommunications Act and the GDPR.

15.2.1 Video identification

In the digital age, there is an increasing demand for secure identification possibilities which do not require personal presence but can be handled online. Business enterprises, such as online banks, but also public authorities, rely here on procedures for online identification via video chat. This is convenient, but also poses risks.

Most recently, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (*Bundesnetzagentur*) recognised video identification as an admissible other identification method within the meaning of sec. 11 (1) of the German Trust Services Act (VDG, *Vertrauensdienstegesetz*). This Act

regulates the transposition into national law of Regulation (EU) No 910/2014 (eIDAS Regulation) on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). The eIDAS Regulation provides a common framework for the cross-border use of electronic means of identification and trust services. Electronic identification is based on unique, secure initial identification, which is now possible in some applications in Germany using the Video-Ident procedure. However, the issuance of qualified certificates for website authentication remains excluded. The issuance of qualified certificates for qualified electronic signatures and/or qualified electronic seals is limited to the issue of certificates that can be used only once (so-called ad hoc certificates). Although I welcome these restrictions on the scope of use, the general recognition of video identification sends the wrong signal for possible further uses of video identification.

In my 25th Activity Report, I already recommended that the Federal Government should not permit the use video identification systems for the identification of customers under the Money Laundering Act. Even then, there was no guarantee that the personal data collected would be processed in compliance with data protection regulations. This statement is still valid.

Video identification does not offer the same level of security as identification among personally present persons. Document verification via a video channel is not fully possible with the current state of the art. Therefore, it is even more difficult to distinguish between a genuine and a forged identity document with video identification compared to on-site identification (see also No. 6.1.2). The integrity of the data used for identification is essential for any secure method of identification, but since this cannot be ensured by video identification, I reject this identification method.

Another problem under data protection law is that complete copies of identity documents are made by recording and storing video sequences. These very extensive records of personal data do not fulfil the requirements applicable to the processing of personal data, i.e. the principles of necessity and data minimisation, since more data is stored than would be necessary for identification. This is another argument against video identification.

It goes without saying that due to increasing digitalisation, a secure method for identification among individuals who are not personally present will be needed in the future. The eID function of the ID card or the electronic residence permit offers a secure procedure here. These functions should be used instead of video identification.

15.2.2 Accreditation – a new task

Art. 43 GDPR provides for accreditation of certification bodies. The accreditation procedure forms an essential basis for reliable and trustworthy data protection certification and can thus make a significant contribution to strengthened and uniform data protection throughout Europe. What we now need to do is to effectively design the needed procedures at national level. Certification is one way in which companies or authorities can voluntarily prove that they comply with the data protection requirements of the GDPR when processing personal data. Art. 42 GDPR contains the relevant provisions on the basis of which the Member States are currently working closely together to develop the required mechanisms and criteria. The Article 29 Working Party has already carried out some initial groundwork in this respect. Finalisation of the corresponding directives is currently underway at the European Data Protection Board (EDPB).

The decisive prerequisite for an effective certification procedure is that only those bodies, which have been reviewed with regard to the expertise required and subsequently formally accredited, may issue certifications in accordance with art. 42 GDPR. Art. 43 GDPR therefore provides for accreditation of certification bodies as an interface between public and private action, which is intended to serve the pur-

pose of conformity verification and quality assurance.

During the course of the national implementation of the accreditation procedure, new central tasks have also emerged for German data protection supervisory authorities. Pursuant to sec. 39 of the Federal Data Protection Act, the German National Accreditation Body (DAkkS, *Deutsche Akkreditierungsstelle*) has to decide on accreditation in agreement with the respective competent supervisory authority. The related rules are laid down in the German National Accreditation Body Act (AkkStelleG, *Gesetz über die Akkreditierungsstelle*).

Before the actual accreditation procedure begins, suitable criteria for accreditation must be defined and published in accordance with art. 57 (1) (p) GDPR. At national level, the data protection supervisory authorities of the Federation and the Länder have been working extensively for some time to develop the corresponding requirements. These requirements must then be sent to the EDPB for approval and are closely orientated towards the guidelines on accreditation already adopted there.

The subsequent accreditation steps can be roughly outlined as follows (see also diagram for No. 15.2.2):

The procedure begins with the application phase for programme review, which is initially coordinated by the German National Accreditation Body, where the responsible supervisory authority already receives information about the receipt of an application and all the documents submitted. The certification programme contains the key requirements for the certification process. High-quality certification criteria are a fundamental precondition for the success and reputation of a certificate. It is precisely for this reason that reviewing the programme submitted and the criteria it contains is an important basis for the next steps of the procedure. The German National Accreditation Body first checks whether certain standard requirements (ISO/IEC 17065 and 17067) are met. The data protection supervisory authority then performs a technical examination. If both checks are successful, suitability for accreditation can then be established in this step.

The next step begins with submission of the accreditation application. The documents are once again checked and forwarded to the competent supervisory authority. The core of this phase is an assessment of the certification body by a team of experts. The experts usually first check the documents submitted and then visit the site. The scope and duration of the assessment depend on the complexity of the respective procedure.

Following this, an accreditation committee evaluates the assessment results and decides on whether to grant accreditation. The accreditation committee consists of members of the German National Accreditation Body as well as of competent experts who are members of the public bodies granting authority. If the decision is positive, an accreditation certificate is issued and accreditation is subsequently listed in the list of accredited bodies at the German National Accreditation Body. The real administrative act, i.e. the authority to act as a certification body, is issued by the competent supervisory authority to the body thereby accredited.

Accreditation is usually valid for a term of five years. In order to ensure proof of competence during this term, checks are carried out at defined intervals. The certification body forwards information regarding certificates issued or revoked to the competent supervisory authority. When accreditation expires, a certification body can submit an application for re-accreditation.

Only a robust, transparent and reliable accreditation procedure in conjunction with clear and publicly available certification criteria can ultimately guarantee credible certification and strengthen confidence in the entire certification procedure.

15.2.3 New lists for critical IT procedures

The GDPR requires controllers to assess the risks to the rights and liberties of data subjects arising from the planned processing of personal data. If this assessment suggests that data processing entails a high risk to the rights and liberties of the data subjects, for example, because particularly sensitive data is involved, controllers are obliged to carry out a detailed assessment of these consequences and to document their results in a so-called data protection impact assessment. For certain classes of processing activities, the GDPR itself already stipulates that a data protection impact assessment must always be carried out for such classes, for instance, in the case of a systematic and extensive monitoring of publicly accessible areas. The GDPR also requires data protection supervisory authorities to establish a list of processing operations beyond those already listed in the GDPR itself and a data protection impact assessment must always be carried out for such processing operations ('blacklist'). In as far as the processing operations in question are of a 'cross-border' nature, for instance, because they form part of a range of goods or services intended for persons from multiple EU Member States, the list must be submitted to the European Data Protection Board (EDPB) which may issue an opinion on the list and, if necessary, request amendments to it. The aim is to ensure uniform application of the GDPR in all EU Member States within the framework of the so-called coherence procedure.

Even before the GDPR came into effect, the European data protection supervisory authorities had already set up a guidance document within the framework of the Article 29 Working Party. These guidelines list nine characteristics that can lead to a high risk to data subjects (see also the criteria for a data protection impact assessment). Where two of these criteria apply to a processing operation, the controller must normally assume that the processing operation involves a high risk to data subjects and is therefore obliged to carry out a data protection impact assessment. For my own 'blacklist', which covers the public area of the federal administration, I directly adopted the procedure from Working Paper 248.

In spring 2018, the German data protection supervisory authorities started to draw up a common 'blacklist' for processing activities in the non-public area. The criteria from Working Paper 248 were chosen as the baseline criteria, but the common 'blacklist' of the German data protection supervisory authorities consists of a list of specifically described types of processing activities. This common list of the German data protection supervisory authorities has now also become the basis for the coherence procedure in the EDPB and has been slightly adapted in the light of the EDPB comments.

After 25 May 2018, as the date when the GDPR came into effect, the majority of the other European data protection supervisory authorities, in addition to their German peers, also initiated the coherence procedure for their respective 'blacklists'. The evaluation of the lists and the preparation of the EDPB's comments were carried out by an EDPB sub-group. As the most important result of this process, the EDPB confirmed that the existing guidance document, i.e. Working Paper 248, was also applicable to the 'blacklists' of the European data protection supervisory authorities and that each element of such list must have two of the characteristics defined in Working Paper 248. Furthermore, a 'common core' of risk factors was agreed to and must be incorporated by each data protection supervisory authority into their 'blacklist' in order to achieve the most uniform possible application of the GDPR in Europe. This concerns the processing of biometric or genetic data, in each case together with another criterion from Working Paper 248.

The guidelines of Working Paper 248, together with the relevant 'blacklists', provide relatively reliable guidance for controllers when it comes to determining whether the proposed processing of personal data poses a high risk to the rights and liberties of data subjects. Notwithstanding this, it should be pointed out once again at this point that a new check must be carried out for each

planned processing activity in order to determine whether a high risk exists. It is quite conceivable that even processing activities, which at first glance do not fulfil any of the criteria laid down in Working Paper 248 and which are not contained in any of the 'blacklists', may nevertheless constitute a high risk. The current versions of the lists are available on my website at www.datenschutz.bund.de .

No significant practical experience with both the criteria of Working Paper 248 and the 'blacklists' is as yet available. New technological developments and business models may lead to a change in the notion of a potentially high risk associated with the processing of personal data. Both Working Paper 248 as the guideline document and the 'blacklists' based on it are therefore likely to be revised at certain intervals. I will closely monitor developments in this area and actively participate in the relevant review processes.

Criteria for a data protection impact assessment

The document "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" (WP 248) sets out the following nine criteria for determining that the processing of personal data involves a high risk to data subjects:

- → Evaluation or scoring
- → Automated-decision making with a legal or similarly significant effect
- → Systematic monitoring
- → Sensitive data or data of a highly personal nature
- → Data processed on a large scale
- → Matching or combining datasets
- → Data concerning vulnerable data subjects
- → Innovative use or application of new technological or organisational solutions
- → Processing in itself prevents data subjects from exercising a right or using a service or a contract

When two of these criteria apply to a processing operation, the controller must normally assume that the processing operation involves a high risk to the rights and liberties of data subjects and should therefore carry out a data protection impact assessment.

However, the respective 'blacklists' are the binding documents:

If a processing activity is included in the 'blacklist' of the data protection supervisory authority responsible for a controller, the latter is always obliged to carry out a data protection impact assessment.

15.2.5 Digital business models using mobile phone data

Digital business models based on the use of mobile data must be re-assessed under the GDPR. The analysis of digital data allows numerous conclusions to be drawn with regard to the behaviour of data subjects. Traffic data – and especially location data – from mobile devices is particularly informative. The information obtained can be used and exploited in a variety of ways for commercial purposes. It is, for example, conceivable to use location data to analyse traffic flows or for statistical purposes (see 22nd Activity Report No. 7.8).

Many opportunities, but also many risks

However, the evaluation of such sensitive data also poses risks. This is particularly true in the context of Big Data where different data can be linked and evaluated in large quantities. Valid anonymisation techniques can be used in order to reduce the associated risks. Furthermore, anonymous and anonymised data is not covered by the scope of European data protection law. However, as the Article 29 Working Party stated in its opinion of 10 April 2014, it is very difficult to generate a truly anonymous database from a comprehensive set of personal data (Working Paper 216, p. 3).

Anonymous is not the same as anonymous!

The decisive factor here is how high the risk of re-identification is (see 25th Activity Report No. 8.8.4; 26th Activity Report No. 17.2.4.4), whereby according to recital 26, 5th sentence of the GDPR both the technologies available at the time of processing and technological developments must be taken into account. In view of rapid technical progress, the effectiveness of existing anonymisation techniques must be permanently checked. The challenge for both controllers and supervisory authorities is to maintain the necessary overview of current technical developments.

Digital business models must meet the requirements of current legislation

The legal requirements for sufficient anonymisation must be reassessed under the GDPR. The same applies to the question as to whether the use of anonymisation techniques as such constitutes processing of personal data and therefore requires a legal basis. I saw the coming into effect of the GDPR and/or the associated change in the legal situation as an opportunity to put the digital business models based on the use of mobile communications data to the test. Furthermore, I initiated a debate among the German supervisory authorities in order to ensure the uniform application of applicable legal provisions in this respect too.

15.2.6 Use of messenger services

Todays' telecommunication services must not only be mobile, but also increasingly faster. Messenger services are very popular for this purpose. Data protection of providers and users of the apps is often forgotten. Messenger services are becoming increasingly popular and have become an integral part of our everyday lives. Companies, in particular, increasingly resort to messenger services in order to communicate with customers (see No. 7.1.5 above).

As already indicated in the 26th Activity Report (No. 17.3.1), my legal view is that messenger services are telecommunications services in the form of so-called OTT (over-the-top) services where communications between participants take place via the open Internet without a dedicated infrastructure. Such services as equivalents to 'classic' telecommunications are subject to the Telecommunications Act and the GDPR with regard to the relationship between the service provider and user. Pursuant to sec. 115 (4) of the Telecommunications Act, my authority is responsible for supervising data protection in Germany (see No. 15.1.1), so that I repeatedly had to deal with the subject of messenger services in the past.

In recent years, there has been a strong focus on the WhatsApp service. In May 2017, I lodged a complaint with the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (*Bundesnetzagentur*) regarding the transfer of user data by WhatsApp Inc. to Facebook. The reason for the complaint was that I was unable to find any user consent to the transfer of the mobile phone number from WhatsApp Inc. to Facebook that was valid under data protection law. I assessed this as a violation sec. 95 (1) 1st and 3rd sentence and sec. 94 of the Telecommunications Act in conjunction with sec. 4a of the Federal Data Protection Act (old). The complaint and the subsequent administrative procedure carried out by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway were not finally processed there. Finally, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway returned the case to me in August 2018 with a reference to the GDPR, even though administrative procedure had not yet been completed. In my opinion, however, it would have been the duty of the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway to make a final statement regarding the WhatsApp complaint procedure and to inform me of the result, because in this respect the legal situation before 25 May 2018 and the violation of sec. 95 (1) 1st and 3rd sentence of the Telecommunications Act in conjunction with sec. 4a of the Federal Data Protection Act (old) is the relevant basis.

My current view is that WhatsApp as the most commonly used messenger service is not data protection-friendly. The potential data exchange between WhatsApp and Facebook is particularly questionable. This also applies to the collection of telephone numbers by WhatsApp using address book uploads. In this way, the company can process all of a user's contact data stored on their mobile phone, regardless of whether or not the contact uses WhatsApp.

I have received several complaints and inquiries regarding WhatsApp. On the one hand, these concern the data protection provisions of the service in general, but also requests for information which were not or only insufficiently answered as well as the question as to how objections can be lodged against the transfer of data, etc.

Messenger services since the coming into effect of the GDPR

Since the most popular messenger services often have neither their headquarters nor a branch in Germany, I have been working intensively with the data protection supervisory authority in charge since 25 May 2018 whenever the processing of stock data subject to the GDPR is involved. This can be illustrated by the following example: If a citizen contacts me because of a data protection problem and the provider is, for example, based in the US, but has a branch in Ireland, as in the case of WhatsApp Ireland Ltd., I take over the correspondence with the lead supervisory authority in the so-called cooperation procedures (art. 56, 60 GDPR) and provide it with all relevant information. The lead supervisory authority then analyses, examines and evaluates the case. It does not only receive my opinion as the supervisory authority concerned, but usually also requests the company concerned to comment in order to make a decision on the basis of these findings. Before taking a final decision, the lead supervisory authority informs me and submits a draft opinion.

If the complaint is successful, I then inform the complainant of the decision taken. If I do not agree with the intended decision, I can appeal against it. The lead authority then has to deal with my arguments and if it upholds its view, it may not issue the decision, but must refer the case to the European Data Protection Board which will then issue a binding decision.

In this way, the supervisory authorities throughout Europe coordinate their activities – usually via the European Internal Market Information System (IMI) – in order to achieve a uniform level of data protection. Needless to say, the high degree of co-ordination is initially a very complex and time-consuming process. Especially during the first months after the GDPR had come into effect, I often saw just how much the devil is in the details of the administrative processes. Over the course of time, however, a certain administrative practice develops in this area too, so that the co-operation procedures for complaints are now gradually gaining ground. The vast majority of the procedures relate to co-operation with the Irish supervisory authority. But my Irish colleague is truly not to be envied, because many large American corporations have their European branch in Ireland and it's easy to imagine how many requests for co-operation from all over Europe have to be handled by the employees there.

Which messenger service should I use?

This is a question I have been asked countless times in recent months. Various service providers offer different messenger services. Which service should one choose then? Which service do the members of one's own social environment use? Which service is secure and data protection-compliant or which one is not? Which service runs on my devices (smartphone, tablet or laptop and PC)? It is a fact is that the best-known and most widely used Messen-

ger service both in Germany and throughout Europe is Whatsapp from Facebook. However, this does not mean that there are no alternative products in terms of functionality or data protection. The most common messenger services include Hoccer, Line, Signal, SIMSme, Skype, Telegram, Threema, Viber and Wire. The decision in favour of or against a messenger service, however, can ultimately only be made by each individual or by the employer in the working environment. After all, the messenger service that meets the requirements best always depends on the individual purpose of use and the resulting requirements for confidentiality, encryption, data security, erasure periods, etc. And what unfortunately also applies to this case is that as long as the e-privacy Regulation (see No. 15.1.2) has not been adopted, many legal issues relating to confidential electronic communications remain unresolved.

15.2.7 Data protection and social media

Scandal upon scandal, and yet the use of social media is becoming more and more widespread. As the supervisory authority, I am called upon here in many respects.

Scandal: What do I care about data protection?

A large number of social media data scandals surfaced during the reporting period. One particularly sensational case was that of Cambridge Analytica, in which data from Facebook users flowed off illegally. During this period, I informed several Bundestag committees about my assessment of the incident in terms of data protection law both during meetings and in writing. As if this scandal were not enough, the so-called Facebook hack became known in September 2018, with hackers capturing millions of user data. In December of the same year, a further security gap was reported that allowed app developers to access user images and private messages for a limited period of time.

As far as data protection is concerned, other social media are not paragons of virtue either. Google failed to disclose a data leak at Google+, which had existed since 2015, to regulators and users for six months after its discovery in March 2018. In December 2018, another vulnerability was discovered that allows developers to access personal data of Google+ users. In May 2018, the microblogging service Twitter was hit by a serious data mishap when it turned out that user passwords were stored in plain text. Finally, a gross breach of data protection also occurred with the Instagram online service which belongs to Facebook. The so-called GDPR tool, which was intended to enable users to view their stored data, displayed their own user password unencrypted in the web address, so that it could also be read by third parties.

New bodies for data protection in social media

The Facebook data scandal in conjunction with Cambridge Analytica prompted the Article 29 Working Party to set up a Social Media Working Group in April 2018 which now continues its work as a sub-working group of the European Data Protection Board and, in addition to the operators of social media, will also look at other stakeholders, such as app developers or data brokers. To these ends, the Social Media Working Group pursues a holistic approach to social media.

Social media and the federal authorities

During the period under review, I also

addressed the use of social media by the public bodies of the Federation for which I am responsible because the use of such communication channels is also increasingly popular there. It is undisputed that authorities must also be represented externally using appropriate media. Citizens ask for these services and expect to be able to access up-to-date information through a variety of channels. However, this must not be at the expense of user privacy.

In view of the many serious data protection incidents in social media, as well as the risk of being legally responsible for data protection violations (see No. 15.2.8 below), I advise the public authorities of the Federation to critically question the need to use social media. Important information may not be provided exclusively via social media. Sensitive personal data has no place in social media. Public authorities themselves should not post such data, nor should they encourage citizens to disclose such data there. A negative example is, for example, when refugees communicate with authorities via their Facebook fanpages and describe their history of persecution in a way everyone can see. For confidential communications, there are more appropriate, secure communication channels to which reference should be made, such as SSL-encrypted forms, encrypted e-mails or De-Mail.

Additional information regarding data protection in social media can be found on my website at www.datenschutz.bund.de .

I advise the public authorities of the Federation to critically question the need to use social media. Important information should not be provided exclusively via social media. Sensitive personal data has no place in social media. Public authorities themselves should not post such data, nor should they encourage citizens to disclose such data there. For confidential communications, there are more appropriate, secure communication channels to which reference should be made, such as SSL-encrypted forms, encrypted e-mails or De-Mail.

15.2.8 ECJ refers fanpage operators to their obligations

At the beginning of June 2018, the European Court of Justice (ECJ) issued a groundbreaking ruling on data protection responsibility in conjunction with the operation of Facebook fanpages (ECJ, ruling of 5 June 2018, Case No. C-210/16). A Facebook fanpage is a kind of homepage that is set up by fanpage operators, such as federal authorities, and published (hosted) by Facebook. Fanpage operators can use the fanpages to present themselves to Facebook users and people who visit the fanpage, and to publish statements of all kinds on the media and opinion market. When visitors access Facebook fanpages, their personal data is processed, also due to the use of cookies. Facebook uses some of this data for its own purposes, but also makes the results of processing available to fanpage operators in the form of a configurable statistics function ('Page Insights'). The ECJ ruled that fanpage operators are jointly responsible with Facebook for processing in conjunction with fanpages. This was preceded by a referral by the Federal Administrative Court to the ECJ in proceedings between Wirtschaftsakademie Schleswig-Holstein GmbH and the Independent Centre for Data Protection of Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*). To the extent that joint responsibility is sufficient, fanpage operators must accept their own liability for data protection violations by Facebook. Furthermore, fanpage operators are obliged to conclude a joint responsibility agreement with Facebook that determines which of the two fulfils which obligations under the GDPR (art. 26 GDPR). In a 'Fanpages' taskforce specifically set up for this purpose, the data protection authorities of the Federation and the Länder are are thoroughly addressing this topic, the

consequences of the ECJ ruling and the implementation measures taken by Facebook in the meantime. I am of the opinion that fanpage operators must guarantee the legality of the data processing for which they are jointly responsible and prove compliance with the principles governing the processing of personal data (art. 5(1) GDPR). In order to be able to assess whether the processing under their own responsibility is carried out in a legally compliant manner, fanpage operators need further information in addition to the information provided by Facebook. Here I see an obligation not only on the part of Facebook to provide further information, but also on the part of fanpage operators to actively request the required information. The same applies to the conclusion of an agreement on joint responsibility that meets the requirements of art. 26 GDPR. The list of questions from the resolution of the data protection conference of 5 September 2018 can serve as an orientation aid for the points to be clarified with Facebook (see box for No. 15.2.8).

As long as these issues have not been resolved with Facebook, I recommend that fanpage operators check whether the operation of a Facebook fanpage is absolutely necessary for them to perform their tasks or whether they cannot – at least until the situation has been clarified – focus on more data protection-friendly communication channels. Federal authorities should be particularly sensitive to this.

I recommend that federal authorities who operate a fanpage check whether the operation of a Facebook fanpage is absolutely necessary for them to perform their tasks or whether they cannot – at least until the legal situation has been clarified – use more data protection-friendly communication channels.

List of questions

- In what way do you and other jointly responsible parties determine which one of you fulfils which obligation in accordance under the GDPR? (Art. 26 (1) GDPR)
- On the basis of which agreement have you determined among yourselves who fulfils which information obligations pursuant to art. 13 and 14 GDPR?
- How are the essential aspects of this agreement made available to the data subjects?
- How do you ensure that the rights of data subjects (art. 12 et seqq. GDPR) can be fulfilled, in particular, the rights to erasure pursuant to art. 17 GDPR, to restriction of processing pursuant to art. 18 GDPR, to object pursuant to art. 21 GDPR and the right of access pursuant to art. 15 GDPR?
- For which purposes and on what legal basis do you process the personal data of visitors to fanpages? Which personal data is stored? To what extent are profiles created or enriched based on visits to Facebook fanpages? Is personal information even of non-Facebook members used in order to create profiles? What periods are planned for erasure?
- For which purposes and on what legal basis are entries in the so-called local storage created even for non-members accessing a fanpage for the first time?
- For which purposes and on what legal basis are one session cookie and three cookies with lifetimes between four months and two years stored after a subpage within the fanpage offering has been accessed?
- Which measures have you implemented in order to fulfil your obligations under art. 26 GDPR as joint controllers and to conclude an appropriate agreement?

17 From my office

17.2 Tasks and establishment of the single contact point

Pursuant to art. 51 (3) in conjunction with recital 119 of the GDPR, Germany, as a Member State with several data protection authorities, is obliged to establish a single contact point that ensures the effective participation of all German supervisory authorities and smooth co-operation with the European authorities in the procedures of the GDPR. Since the German legislator had assigned the function of the single contact point to my authority, the necessary organisational prerequisites had to be created during the reporting period.

Tasks and establishment in detail:

The single contact point (art. 17 (1) GDPR), which I have set up but which is organisationally separate, operates in the common interest of the 18 supervisory authorities of the Federation and the Länder. It acts as a link between these 18 supervisory authorities on the one hand and the supervisory authorities of the other Member States, the European Data Protection Board (EDPB) and the European Commission on the other. For this purpose, the single contact point forwards all information and communications which it receives to the German supervisory authorities concerned. Conversely, the German supervisory authorities can use the single contact point for cross-border communications with the aforementioned bodies. Furthermore, the single contact point is especially designed to enable EU institutions and the supervisory authorities of other Member States to effectively communicate with the German supervisory authorities without knowledge of the distribution of national responsibilities. One of the most important tasks of the single contact point is to coordinate the definition of common positions of the German data protection authorities in European matters (see No. 17.3). The single contact point also carries out other supporting tasks, such as monitoring deadlines for co-operation and coherence procedures according to the GDPR, identifying contact persons, accompanying people to meetings in Brussels or providing organisational support for the registration of German representatives for EDPB meetings and its working parties. However, the single contact point does not carry out any sovereign administrative tasks in relation to citizens, authorities and companies and does not take any action in relation to these.

The Internal Market Information System as a tool for co-operation between German and European supervisory authorities

The data protection supervisory authorities involved use the Internal Market Information System (IMI) in order to coordinate cross-border cooperation and coherence procedures under the GDPR. IMI is an application on the Internet that connects all European and German data protection supervisory authorities across borders. This enables quick and easy communications between the connected authorities and ensures cooperation between European administrations. The system is managed at European level by the Secretariat of the EDPB which has set up a dedicated IMI helpdesk. The legal basis for the implementation of the programme is European Regulation No 1024/2012 of 25 October 2012 and an implementing act. The aforementioned Regulation also regulates the rights of data subjects and provides, for example, for special rights of access and erasure. In terms of data protection law, I already examined the system in December 2012, albeit in relation to another specialist application, without raising any objections (see 24th Activity Report No. 2.3.1). In co-operation with the European Commission and in consultation with representatives of the Member States, separate input forms were created for the new cross-border procedures under the GDPR in order to ensure that only the data required in each case will be collected.

17.8 Events

As an organiser of symposia, a new specialist focus is set every year as part of public relations work. Other events are designed to inform citizens about various topics relating to data protection. During the reporting period, I organised two specialist events. At the 2017 'Symposium on Data Protection in Automated and Interconnected Cars' (*Symposium zum Datenschutz im automatisierten und vernetzten Auto*), an important topic for the future was discussed with experts from politics, business and civil society (see No. 1.6). Just as important was the dialogue conference on the exercise of data protection rights by children, which I organised in 2018 together with the 'Germany Secure on the Internet' (DSiN, *Deutschland sicher im Netz e. V.*) initiative and the Association of Data Protection Officers (BvD, *Berufsverband der Datenschutzbeauftragten Deutschlands*) (see No. 1.7).

In addition to these symposia, my authority successfully participated in the Federal Government's Open Day in Berlin in 2017 and 2018. My staff and I provided information on various aspects of data protection and freedom of information and had many interesting talks with citizens.

17.8.1 Event on Binding Corporate Rules

In June 2017, the Federal Commissioner for Data Protection and Freedom of Information hosted an international workshop for European data protection supervisory authorities on 'Binding Corporate Rules'. Within global corporations and groups, personal data is also transferred to group companies based in countries in which the data protection regulations of the EU do not apply (so-called third countries). In order to provide adequate protection for personal data in such cases too, appropriate safeguards, in particular, appropriate guarantees, must be provided. Such guarantees usually consist of companies issuing binding corporate rules (BCRs) to each other. At the international workshop, experts from various supervisory authorities coordinated and further developed the content requirements for BCRs to be fulfilled by the companies as well as the processes for their Europe-wide recognition.