

Activity Report 2019

28th Activity Report
on Data Protection



BfDI

Federal Commissioner
for Data Protection and
Freedom of Information



This report was presented to the President of the German Bundestag, Dr. Wolfgang Schäuble.

Federal Commissioner for Data Protection
and Freedom of Information
Prof. Ulrich Kelber

Foreword

According to the General Data Protection Regulation (GDPR), each independent data protection supervisory authority must draw up an annual report on its activities. In keeping with this requirement, the 28th Activity Report on Data Protection covers the year 2019.

The report highlights the most important areas of (data protection) policy that occupied the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) in 2019. It also contains updates on consultations and controls carried out in Germany, details of the ever-closer cooperation between European supervisory authorities on GDPR implementation within the

European Union, and a range of different statistics on the BfDI's work.

In addition, the report provides an overview of progress made in relation to implementing the recommendations issued by the BfDI in previous years.

The 28th Activity Report will also be the last report by the BfDI devoted solely to the topic of data protection. From the reporting period 2020 onwards, the BfDI's activity reports will encompass both data protection and freedom of information.

Communication

by the Federal Commissioner for Data Protection and Freedom of Information

2019 Activity Report on Data Protection
– 28th Activity Report –

Table of Contents

Inhalt

- Foreword** 2
- Table of Contents 3
- 1. Introduction** 6
- 2. Recommendations 8
 - 2.1 Summary of the recommendations made in this activity report 8
 - 2.2 Recommendations made in the 27th Activity Report – implementation status 9
 - 2.3 Recommendations from previous activity reports – implementation status 12
- 3. Committee work** 14
 - 3.1 Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany (DSK) 14
 - 3.2 European Data Protection Board (EDPB) 19
 - 3.3 Data protection committee of the Council of Europe 21
 - 3.4 International Conference of Data Protection and Privacy Commissioners 21
- 4. Main Topics** 23
 - 4.1 Evaluation of the GDPR 23
 - 4.2 Digitalisation in the healthcare sector 24
 - 4.2.1 Telematics infrastructure and its applications 25
 - 4.2.2 Implant register 26
 - 4.3 Data minimization 27
 - 4.4 Artificial intelligence 29
 - 4.5 Consent under data protection law 31
 - 4.5.1 Consent to research 31

4.5.2 Tracking and cookies	32
4.6 Opinion of the Data Ethics Commission.....	32
5. Legislation	37
5.1 The Omnibus Act on the General Data Protection Regulation	37
5.2 Further wait for amendments to the Telecommunications Act.....	38
5.3 Security legislation	39
5.3.1 Customs Investigation Service Act.....	40
5.3.2 Code of Criminal Procedure.....	40
5.3.3 The dark web.....	41
5.4 Census 2021	41
5.5 Modernisation of registers within Germany.....	42
5.6 Legislation in the field of healthcare and social welfare	43
6. Security	46
6.1 Cross-border access to data by the security authorities	46
6.1.1 CLOUD Act	46
6.1.2 The eEvidence Regulation.....	46
6.1.3 Convention on Cybercrime	47
6.2 “Smart” video surveillance pilot project at Berlin-Südkreuz railway station	47
6.3 Police 2020.....	48
6.4 Storage of PNR data	49
6.5 Queries submitted to the BfV before awards of public funding	50
6.6 Advisory and fact-finding visits to the Federal Intelligence Service.....	51
6.7 Controls involving the security authorities	51
6.7.1 Mandatory controls	51
6.7.2 Source telecommunications surveillance within the BKA.....	53
6.7.3 The BKA’s handling system	54
6.7.4 Data protection and security clearances	55
6.7.5 Fragmentation of the supervisory landscape for the intelligence services	56
7. Bundestag	58
7.1 The Bundestag’s internal pass and access system.....	58
7.2 Controls in relation to the Bundestag police.....	58
8. Other individual topics	59
8.1 Third-country transfers.....	59
8.1.1 Consequences of Brexit for data transfers	59
8.1.2 Proceedings in the Schrems II case	59
8.1.3 Developments relating to the EU-US Privacy Shield	60
8.2 The Online Access Act.....	60
8.3 Unencrypted e-mails.....	62
8.4 Misuse of data by the Federal Employment Agency’s Job Board.....	63

8.5 Legislation on aliens and asylum.....	64
8.6 Facebook fanpages	64
8.7 Data protection in motor vehicles.....	65
8.8 Data protection and postal services	67
8.8.1 Digital Copy.....	67
8.8.2 Carrier sequence sorting for increased delivery efficiency.....	68
8.9 Fining methodology issued by the data protection authorities.....	68
8.10 Green light for accreditation	70
8.11 Federal IT Consolidation Project.....	71
8.12 Data protection and Windows 10	72
9. Internal developments within the BfDI	74
9.1 Staffing changes and internal organisation.....	74
9.2 Public outreach work.....	74
9.3 The BfDI's work in figures.....	76
10. BfDI as the Single Contact Point.....	80
10.1 Cooperation between the national supervisory authorities on European topics.....	80
10.2 Statistical overview of cooperation and cohesion procedures at European level from the perspective of the Single Contact Point.....	81
Keyword directory	83

1. Introduction

The topic “Artificial intelligence” (AI) and its significance for data protection was a major focus of my work in 2019. The Conference of the Independent Federal and State Data Protection Supervisory Authorities (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, DSK) presented a statement of principles setting out key requirements relating to data protection law – the “Hambach Declaration on Artificial Intelligence” – in which, alluding deliberately to the demands for freedom and democracy made at the Hambach Festival in 1832, it emphasises that the use of artificial intelligence must be accountable to human beings and their fundamental rights and freedoms (see No. 3.1).

These same principles were also enshrined in the opinion of the Data Ethics Commission (Datenethikkommission, DEK) set up by the Federal Government, of which I was a member. The DEK furthermore issued 75 recommendations for action by the Federal Government, calling among other things for greater transparency for consumers and effective controls of algorithms (see No. 4.6).

Artificial intelligence was also one of the topics identified as a key area of work over the coming years at the 41st International Conference of Data Protection Authorities, which took place in October 2019 in Tirana (Albania). The independent data protection authorities attending the conference – around 120, from over 80 countries – adopted a “Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights”, calling on governments around the world to recognise data protection as a fundamental right and to enshrine it in their national legislations (see No. 3.4).

Moving away from the topic of AI, in 2019 it became clear once again that data protection is a cross-sectoral issue that impacts all areas of life, meaning that the volume of work was as high as ever. Within Germany’s borders, my staff and I were mainly kept busy with legislative consultations and oversight of

legislative processes. In addition to the Omnibus Act on the GDPR – and the renewed proliferation of legislation concerning the security authorities – the healthcare sector was a particularly rich source of work this year. The German Federal Ministry of Health (Bundesgesundheitsministerium, BMG) alone tabled 23 bills, some of which posed a serious threat to the tenets of data protection legislation.

Examples include the ongoing problems concerning the telematics infrastructure and rights management for the electronic health record; the in-depth consultations on these issues occupied a great deal of my co-workers’ time. The BMG is keen to introduce the electronic health record as quickly as possible and across the board, but this entails the risk of abandoning long-established and fundamental data protection rules, with potentially disastrous consequences for patients in an area that involves handling highly sensitive data.

In my opinion, the procedures for handling patient data in the planned new health registers (implant register and data transparency register) also need tightening up in many respects; a large number of consultations were therefore held with the parties involved in designing these procedures (see No. 4.2 and No. 5.6).

Aside from providing advice to the Federal Government and the Bundestag on legislative matters, a large part of my time is taken up by consultation and control activities involving the authorities and undertakings under my oversight. As far as I am concerned, priority should always be placed on the provision of advice and information, and this is doubtless one of the reasons why the GDPR treats the imposition of fines for breaches of its provisions as an exception rather than a rule.

Nevertheless, I was obliged to impose hefty fines for the first time in 2019.

Consent to data transfers and data minimisation are topics that recur on a regular basis, particularly in citizen complaints.

Consent to the transfer of data is a multi-faceted and thorny issue, particularly in the field of research, but one that we encounter on a daily basis whenever an irksome cookie banner pops up on a website (see No. 4.5).

The question of which data should be collected in the first place and for how long these data should be retained represents a perennial problem for all data protection supervisory authorities. The steps taken by authorities and undertakings in pursuit of the goal of data minimisation are not always satisfactory (see No. 4.3).

In connection with the evaluation of the GDPR scheduled to be carried out by the European Commission, we made use of our platform within the DSK and the European Data Protection Board (EDPB) to propose improvements to this piece of legislation. Our aims include lightening the load on associations and small undertakings in respect of their information and documentation obligations, establishing better regulations on profiling and scoring, and improving the handling of major cross-border cases (see No. 4.1).

The topic of cooperation between the European supervisory authorities is gaining in importance. Over the course of the year, the EDPB took many key decisions relating to interpretation of the GDPR; some of these decisions laid the groundwork for issuing certifications, for example. Regrettably, I am still waiting – and the citizens are waiting along with me – for the first rulings on data protection complaints against the US Internet giants. Almost all of these companies have their European

headquarters in Ireland or Luxembourg, and cross-border complaints have been pending before the data protection supervisory authorities of these countries for 20 months so far, without any adjudication on their central points. I find this both incomprehensible and more than a little aggravating, and I raise the issue at each of the EDPB's monthly meetings in the hope that we will be able to remedy this regrettable state of affairs together in 2020.

I would like to thank my co-workers for demonstrating a consistently high level of commitment once again. One of the things that emerges clearly from this activity report is the sheer number of areas (both broad and narrow) in which the BfDI is active with a view to protecting citizens' fundamental rights. My co-workers put an enormous amount of enthusiasm into the task of serving as an "advice shop" for the authorities and undertakings under our oversight, as well as for policymakers and the public; they put just as much enthusiasm into the task of performing controls and cooperating within countless different working groups, commissions, committees and organisations at national, European and international level.

Finally, I would like to express my particularly warm thanks to all the citizens who have contacted the BfDI with their requests and queries. They are our partners in the task of data protection enforcement.

Prof. Ulrich Kelber

2. Recommendations

2.1 Summary of the recommendations made in this activity report

I recommend enshrining in law the “principle of explainability” and complying with the seven data protection requirements set out in the “Hambach Declaration on Artificial Intelligence” when implementing artificial intelligence (AI) in a wide range of fields (Nos. 3.1 and 4.4).

In connection with the first evaluation of the GDPR, I recommend backing the position of the national data protection supervisory authorities and the EDPB. This is particularly true in respect of the calls for meaningful steps to reduce the burden of red tape on small and medium-sized enterprises and for a tightening up of the legal framework for profiling (No. 4.1).

I recommend implementing a differentiated system for the management of rights and roles in connection with the electronic health record (No. 4.2.1).

I recommend declaring a moratorium on security-related legislation and launching an evaluation of the powers of intervention granted to the security agencies (No. 5.3).

As regards the modernisation of registers, I recommend using multiple sector-specific identifiers instead of a single personal identification number (No. 5.5).

Given the high error rate and lack of legal basis, I recommend that video surveillance systems based on biometric facial recognition should not be used in public spaces (No. 6.2).

In connection with services under the [German] Online Access Act (Onlinezugangsgesetz, OZG), I recommend that citizens should be provided with a user-friendly opportunity to learn about and monitor the data processing operations that are taking place (No. 8.2).




I recommend that the public authorities of the Federation should always encrypt personal data before sending them by e-mail. It is unlawful to send sensitive data by e-mail without encrypting it first, even if consent to do so has previously been obtained from the recipient, since consent of this kind cannot typically be granted in a manner that complies with data protection requirements. Furthermore, provisions of national law that legitimise the sending of unencrypted e-mails constitute an infringement of the GDPR (No. 8.3).

I recommend that non-discriminatory access should be granted to vehicle data and data generated in vehicles via a secure vehicle-based telematics platform, following the example of smart meter gateways or similar (No. 8.7)

2.2 Recommendations made in the 27th Activity Report – implementation status




Recommendation	Implementation status
 I recommend that the legislator should award the BfDI remedial powers under the new [German] Federal Police Act (<i>Bundespolizeigesetz</i> , BPolG). These should at least correspond to the powers already enshrined in the new [German] Federal Criminal Police Office Act (<i>Bundeskriminalamtgesetz</i> , BKAG) (No. 1.2 of the 27th Activity Report).	<p>The draft of the new Federal Police Act forwarded to the BfDI awards certain remedial powers to the BfDI, following the example of the Federal Criminal Police Office Act. The requirements imposed are more stringent than those provided for by the Directive, however. For example, the provisions state that an order can be issued only in response to a complaint. In addition, no explicit provision is made for erasure orders. This increases the risk that effective remedial action will not be possible.</p>
 I recommend that the legislator should also grant the BfDI the authority to impose sanctions in the area of the intelligence services (No. 1.2.1 of the 27th Activity Report).	<p>The legislator has not yet acted upon this recommendation.</p>
 I recommend that the legislator should clarify that fines for GDPR breaches can also be imposed on statutory health insurance funds if these latter act as commercial enterprises (No. 1.1 of the 27th Activity Report).	<p>The legislator has taken no further action in this respect to date, resulting in uncertainty among the statutory health insurance funds. On the one hand, Section 85a of the [German] Social Code (<i>Sozialgesetzbuch</i>, SGB) (Volume X) states that fines cannot be imposed on authorities and other public bodies. On the other hand, the statutory health insurance bodies act as enterprises governed by public law that are exposed to competition, as per the [German] Act for Fair Competition among Health Insurance Funds (<i>Fairer-Kassenwettbewerb-Gesetz</i>, GKV-FKG) adopted on 13 February 2020 by the German Bundestag. Section 2 (5) of the [German] Federal Data Protection Act (<i>Bundesdatenschutzgesetz</i>, BDSG) states in this respect that public bodies shall be regarded as private bodies if they take part in competition as enterprises governed by public law. Statutory health insurance funds advertise for customers (insured parties) in the same way as private health insurance funds, for example during sports events. Article 83 GDPR applies to enterprises governed by public law that are exposed to competition.</p>
 I recommend that staffing levels within job centres should be increased to the point that they can free up their data protection officers to work solely on data protection tasks, ensuring that they can comply with their requirements under law (No. 3.2.1 of the 27th Activity Report).	<p>Although a small number of job centres have acted upon this recommendation, we are aware that much remains to be done in terms of freeing up data protection officers to work on data protection tasks. This recommendation should therefore be carried forward.</p>

Recommendation	Implementation status
 <p>Having regard to the guidance from the European Court of Justice (ECJ) on the EU-Canada PNR agreement, I recommend that the Federal Government should revise the [German] Passenger Data Act [<i>Fluggastdatengesetz</i>, FlugDaG] and campaign in Brussels for a revision of Directive (EU) 2016/681 (No. 1.3 of the 27th Activity Report).</p>	<p>Several questions of principle relating to the compatibility of the PNR Directive with national PNR laws have been referred to the ECJ for preliminary rulings (including a request by the Belgian Constitutional Court, C 817/19). The German Federal Government believes that the existing provisions are compatible with the Charter of Fundamental Rights of the European Union, in part because they are couched in different terms to the EU-Canada PNR agreement, and in part because they serve a different purpose and are based on a different assessment of proportionality. Amendments are unlikely before these proceedings have reached a conclusion, and in particular before light has been shed on the admissibility of long-term data retention.</p>
 <p>I recommend that the legislator should adopt clear rules of jurisdiction concerning the control activities carried out by the BfDI and the G10 Commission; these rules should also cover cooperation between these two supervisory authorities. I furthermore recommend that the BfDI's authority to carry out controls should be comprehensively recognised, inter alia when working on shared dossiers with the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) regarding foreign intelligence services, and regulated by law if necessary in the interests of clarification (No. 9.1.5 of the 27th Activity Report).</p>	<p>This recommendation had not been followed up on by the editorial deadline for this report. It is not yet possible to gauge the extent to which it will be implemented as a result of ongoing legislative procedures.</p>
 <p>I recommend that the newly developed standard agreement on contract data processing should be used throughout the entire Federal Administration when concluding agreements in respect of contract data processing. The standard agreement is published on my website (No. 9.2.6 of the 27th Activity Report).</p>	<p>The standard agreement is not yet widely used (even as a basis) by the Federal Administration.</p>
 <p>I recommend that police authorities should have access to meaningful documentation when accessing Eurodac and the Visa Information System (VIS) (No. 9.3.5 of the 27th Activity Report).</p>	<p>The bodies responsible have agreed on measures to optimise the documentation, and these measures seem likely to result in improvements. This remains to be confirmed by means of follow-up controls, however.</p>
 <p>In view of their limited practical value, I recommend that the legislator should abolish the anti-terror file (Anti-Terror-Datei, ATD) and the right-wing extremism file (Rechtsextremismus-Datei, RED) (No. 9.3.5 of the 27th Activity Report).</p>	<p>The legislator has not yet followed up on this recommendation.</p>
 <p>I recommend that the [German] Code of Criminal Procedure (Strafprozessordnung, StPO) should be revised. In particular, the collection and use during criminal proceedings of data that have been gathered by informants for police- or intelligence-related purposes should be regulated in such a way as to create legal clarity. Cooperation with the authorities ensuring the protection of the Constitution should in any case be regulated more stringently and in greater detail. The consistent past decisions by the Federal Constitutional Court should be implemented with this in mind (No. 11.1.2 of the 27th Activity Report).</p>	<p>Although amendments were made to the Code of Criminal Procedure on several occasions, none of these legislative procedures resulted in the implementation of this recommendation.</p>

Recommendation	Implementation status
 <p>I strongly recommend that the ePrivacy Regulation should 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 applies, in particular, to the relationship between the [German] Telecommunications Act (Telekommunikationsgesetz, TKG) and the GDPR (No. 15.1.2 of the 27th Activity Report).</p>	<p>The proposal for an ePrivacy Regulation has been under negotiation since 2017, but the EU Council has not yet been able to agree on a general approach. Croatia's Presidency of the Council began in January 2020; on 21 February 2020, an amended proposal was issued by this Presidency.</p>
 <p>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 have 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 (No. 15.2.7 of the 27th Activity Report).</p>	<p>Information is, at the very least, no longer being disseminated exclusively via social media. Individual authorities have demonstrated an awareness of the problem and are examining the use of alternative services.</p>
 <p>I recommend that federal authorities that operate a Facebook fanpage should check whether the operation of the 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 (No. 15.2.8 of the 27th Activity Report).</p>	<p>Facebook fanpages continue to be operated. The information provided by Facebook on its data processing operations still lacks transparency, although improvements have been observed in certain respects. The data protection authorities have stepped up their calls for clarification of the outstanding legal issues at EU level.</p>

2.3 Recommendations from previous activity reports – implementation status

Recommendation	Implementation status
<p> I appeal to federal and state regulators to embrace the spirit and letter of the new European rules when amending national data protection law, with a view to achieving largely uniform European data protection legislation in future (Nos. 1.1, 1.2 et seqq. of the 26th Activity Report).</p>	<p>My recommendation was implemented in part by means of the [German] Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (<i>Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680</i>, DSAnpUG-EU) and the associated creation of a new Federal Data Protection Act. I take a critical view of a number of the provisions of this new Act, however (see No. 1.1).</p> <p>The Second Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, which will bring large swathes of the Federal Government’s sector-specific data protection law into line with the provisions of the GDPR, has now been tabled. I am monitoring this ongoing legislative procedure, and have already highlighted a number of areas that require improvement in the opinion I submitted (see No. 1.1). Most of the points I raised were ignored during the further course of the legislative procedure. For example, the legislator failed to introduce fines for data breaches by statutory health insurance funds– contrary to the original plans – and to carry out the much-needed amendments to the Telecommunications Act.</p>
<p> I recommend that the legislator should make use of the option granted under the GDPR to adopt specific national rules on employee data protection in the near future (Nos. 3.1 and 3.2.1 of the 26th Activity Report).</p>	<p>Although the legislator incorporated a number of provisions on data processing for purposes of the employment relationship into the recast Federal Data Protection Act (Section 26 BDSG), for the most part this involved carrying over the existing provisions of law. There continues to be a need for comprehensive specific rules, and so my recommendation that the legislator should adopt specific national rules on employee data protection remains in place (see No. 3.1.3). Work on the drafting of a corresponding bill has not yet commenced, and the advisory board planned for this purpose has not yet been set up.</p>
<p> I recommend that the legislator should make use of the discretion granted to it under the GDPR in the field of statutory health insurance and preserve the foundations of the carefully balanced structure of sector-specific provisions of data protection law (No. 9.1 of the 26th Activity Report).</p>	<p>In the [German] Act amending the Federal Law on War Pensions and other Regulations (<i>Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften</i>) of 17 July 2017 (Federal Law Gazette I, p. 2541), the legislator made amendments to the basic provisions on social data protection in Chapter 2 of SGB Volume X with a view to bringing them into line with the GDPR, but failed to adopt provisions that would deliver better outcomes not only for insured persons, but also for the social security administration and the research community, in keeping with the GDPR (see No. 7.1.1). The intended purpose of the Second Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 is to adapt the sector-specific volumes of the Social Code to the provisions of the GDPR, but only editorial amendments are planned. This falls short of what is needed to preserve the carefully balanced framework of sector-specific provisions of data protection law concerning the statutory health insurance funds.</p>

Recommendation	Implementation status
 <p>I recommend that the legislator should ensure that the necessary conditions are in place to carry out effective data protection supervision in the area of the security authorities and the intelligence services, in line with the compensatory function called for by the Federal Constitutional Court, and that it should respond to the urgent need to increase staffing levels within the BfDI yet further. Efficient measures to guarantee security and effective data protection controls are two sides of the same coin. Action by the budgetary legislator is still needed in this area (No. 1.3 of the 26th Activity Report).</p>	<p>I am pleased to report that the budgetary legislator implemented my recommendation. The BfDI was granted funding for 44 additional posts in the area of security under the 2019 and 2020 budgets. I hope that future budgets will also take into consideration the need to increase the staffing levels of the bodies responsible for data protection supervision every time that the security agencies are granted extra competences or receive funding for additional posts.</p>
 <p>I recommend that the legislator should ensure that the legal basis for granting powers of intervention to the security agencies and the intelligence services is constitutionally compliant in accordance with the requirements laid down by the Federal Constitutional Court in respect of the Federal Criminal Police Office Act, e.g. by amending the relevant provisions accordingly (No. 1.3 of the 26th Activity Report).</p>	<p>This recommendation has not yet been implemented for the most part. At this stage, it is not possible to gauge the extent to which it will be implemented as a result of ongoing legislative procedures.</p>
 <p>I recommend that the legislator should adopt legislative provisions on the introduction of mortality registers for research purposes (No. 9.2.3 of the 26th Activity Report).</p>	<p>I regret to say that the legislator has not yet taken any action in this respect.</p>
 <p>I recommend that the legislator should adopt clear guidelines on IT systems with a view to making these systems as secure and resilient as possible while, at the same time, ensuring the highest possible level of protection for personal data (No. 10.2.11.1 of the 26th Activity Report).</p>	<p>Although the draft IT Security Act 2.0 was published in spring 2019, no further action was taken in this respect during the rest of the year. I hope that future legislative initiatives will take into account my concerns about the significant tightening up of criminal law and criminal procedural law. It is important to expand further the protections available to society and the economy in the digital world, but this must happen in a way that does not impinge on data protection.</p>

3. Committee work

3.1 Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany (DSK)

The DSK, which was chaired this year by the Rhineland-Palatinate State Commissioner for Data Protection and Freedom of Information, adopted a new short paper, nine resolutions and 11 decisions during two ordinary data protection conferences and three interim conferences.

2019 was a busy year for the independent data protection supervisory authorities of the Federal Government and the Länder. Although the GDPR entered into force on 25 May 2018, many matters still require coordination between the supervisory authorities. Topics are discussed and fundamental positions adopted within the DSK with a view to achieving maximum harmonisation of its approach to points of data protection law, with a particular focus on topics that require cooperation by the supervisory authorities at national or international level. Ad-hoc debates are also held on topical and fundamentally important questions of data protection law that require further clarification. The DSK has set up working groups that support its activities in these areas.

Hambach Declaration

Key issues discussed at the 97th Conference of the Independent Federal and State Data Protection Supervisory Authorities at Hambach Castle in Neustadt an der Weinstraße included the requirements under data protection law for the development and use of artificial intelligence and corporate liability under Article 83 GDPR for culpable data breaches by a company's employees.

The Hambach Declaration sets out seven data protection requirements that should be observed during the technical development and use of artificial intelligence in all the various spheres of life.

In-house data protection officers and exchanges of information with specific supervisory authorities

The DSK also adopted a resolution setting out its position on the legal status of in-house data protection officers, in response to critical comments from several quarters about the fact that too many companies are obliged under the GDPR to appoint a data protection officer. The DSK does not share the sentiments behind these comments. The provisions of the GDPR imposing an obligation to appoint a data protection officer have not resulted in any substantive changes to the provisions of data protection law that previously applied. Instead, a failure to appoint a data protection officer would simply have increased a controller's workload, since the guidance provided by data protection officers and the controls they carry out are indispensable for any controller seeking to fulfil the obligations imposed by data protection law.

The DSK broadened the scope of its exchanges of information with specific supervisory authorities representing media and religious groups as a basis for cooperation with the EU's data protection bodies.

Number plate recognition and digitalisation in the healthcare sector

The topics examined by the 98th DSK in Trier included large-scale automatic number plate recognition systems and the processing of personal data in the healthcare sector.

The DSK believes that the large-scale and blanket use of automatic number plate recognition systems for law enforcement purposes constitutes an infringement of the [German] Basic Law (Grundgesetz, GG) and a violation of citizens' right to informational self-determination. Police authorities and public prosecutor's offices should no longer be allowed to use number plate recognition systems on a large-scale and indiscriminate basis for the purpose of logging, storing and evaluating vehicle data, and any data that have been stored unlawfully should be erased.

Resolution of the 97th Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany

Hambach Castle, 3 April 2019

Hambach Declaration on Artificial Intelligence

Seven data protection requirements

Artificial intelligence (AI) systems pose a substantial challenge for freedom and democracy in our legal order. AI developments and AI applications must comply with fundamental rights in a democratic and constitutional manner. Not everything that is technically possible and economically desirable may be allowed to be implemented in reality. This applies in particular to the use of self-learning systems which process data on a massive scale and interfere with the rights and freedoms of those concerned by automated individual decisions. Protection of fundamental rights is a key role of all public powers. Essential frameworks for the use of AI need to be defined by legislators and implemented by supervisory authorities. Only if the protection of fundamental rights and data protection can keep pace with the process of digitalisation, a future is possible in which, in the end, human beings and not machines decide over human beings.

I. Artificial intelligence and data protection

Artificial intelligence is currently being discussed intensively as it promises added value in many areas of business and society. The German Government has published an AI strategy with the aim of making Germany world leader in the development of AI. “AI made in Germany” is, at the same time, meant to ensure that even with far-reaching use of artificial intelligence, the basic values and civil liberties which apply in Germany and in the European Union (EU), will continue to play a significant role in our coexistence. The independent federal and state data protection supervisory authorities explicitly welcome this approach of fundamental rights-compatible design of AI.

A generally accepted definition of the term artificial intelligence has not yet been found. According to the German Government’s understanding, AI is about “designing technical systems in such a way that they can handle problems independently and are able to adapt themselves to changing conditions. These systems’ characteristic is the ability to ‘learn’ from new data.”

AI systems are already being used, for example, in medicine to support research and therapy. Even today, neuronal networks are able to automatically recognise complex tumour structures. AI systems can also be used to detect depression disorders based on behaviour in social networks or based on voice modulation when operating virtual assistants. In the hands of medical professionals, this knowledge can serve the patients’ well-being. In the wrong hands, however, it can also be misused.

An AI system was also used to evaluate job application documents with the goal of deciding free from human prejudices. However, the company had hired predominantly male applicants in the past and the AI system had been trained with their successful applications. Subsequently, the AI system assessed women as being much less qualified even though the gender was not only no predetermined evaluation criterion but also unknown to the system. This reveals the danger of discrimination originating in training data and not being eliminated but rather being solidified.

These examples make clear that AI systems often process personal data and this processing poses risks to the rights and freedoms of people. They also demonstrate how important it is to monitor and regulate development and usage of AI systems politically, socially and legally. The independent federal and state data protection supervisory authorities understand the following requirements as a constructive contribution to this vital socio-political project.

II. Data protection requirements for artificial intelligence

The General Data Protection Regulation (GDPR) includes important legal requirements for development and use of AI systems processing personal data. They aim at the protection of fundamental rights and freedoms of natural persons. The principles relating to processing of personal data (Article 5 GDPR) also apply to AI systems. According to Article 25 GDPR, these principles must be implemented by the controllers through technical and organisational measures planned at an early stage (data protection by design).

1. AI must not turn human beings into objects

The guarantee of human dignity (Article 1 (1) GG and Article 1 of the Charter of Fundamental Rights of the EU) demands that an individual must not be objectified, particularly where AI is being used by public authorities. Fully automated decisions or profiling by AI systems are permitted to a limited extent only. Decisions with legal effect or similar significant interference may not, pursuant to Article 22 GDPR, be left to the machine only. If the scope of Article 22 GDPR is not applicable, the basic principles of Article 5 GDPR still apply which protect individual rights in particular through the principles of lawfulness, fairness and accountability. Even when AI systems are used, those affected have the right to the intervention of a real person, to the presentation of his or her point of view and the right to contest a decision.

2. AI may be used only for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation

AI systems may only be used for constitutionally legitimate purposes. The principle of purpose limitation must also be observed (Article 5(1)(b) GDPR). Article 6(4) GDPR sets clear limits to changes of purpose of personal data processing. Extended processing purposes must be compatible with the original purpose of collection also with AI systems. This applies also to the processing of personal data in AI systems for training purposes.

3. AI must be transparent, comprehensible and explainable

Personal data must be processed in a way that is comprehensible to the data subject (Article 5(1)(a) GDPR). This requires, in particular, a transparent processing which comprises easily accessible and understandable information about the procedures of processing and, if necessary, also about the used training data (Article 12 GDPR). Decisions taken on the basis of the use of AI systems must be comprehensible and explainable. Explainability with regard to the result alone is not sufficient. Comprehensibility with regard to the procedures and the decision-making process needs to be ensured, too. According to the GDPR, the logic involved needs to be explained as well. These transparency requirements are to be fulfilled continuously if AI systems are being used to process personal data. The principle of accountability of the controller (Article 5(2) GDPR) applies.

4. AI must avoid discrimination

Learning systems are highly dependent on the data entered. Insufficient data bases and processing concepts can lead to results with discriminating effects. Discriminating processing is an infringement of the rights and freedoms of the persons concerned. They violate, among other things, certain requirements of the GDPR such as the principle of fairness, the restriction of processing to legitimate purposes and the adequacy of the processing.

Discriminating tendencies are not always apparent from the outset. Therefore, an assessment of risks for the

5. The principle of data minimisation applies to AI

AI systems typically process large amounts of training data. The principle of data minimisation (Article 5(1)(c) GDPR) also applies for personal data in AI systems. The processing of personal data must, therefore, always be limited to what is necessary. Considering necessity may lead to the result that processing of completely anonymous data is sufficient for achieving a specific legitimate purpose.

6. AI needs responsibility

The parties involved in the use of an AI system must determine and communicate clearly who shall be the responsible controller. And, respectively, the controller needs to take the necessary measures in order to achieve lawful processing, to ensure the rights of a data subject, security of the processing and controllability of the AI system. The controller must ensure that the principles of Article 5 GDPR are being complied with. The controller must fulfil the obligations with regard to the rights of data subjects laid down in Articles 12 et seqq. GDPR. The controllers must ensure security of processing in accordance with Article 32 GDPR and, thus, prevent manipulations by third parties which can affect the results of the systems. When using an AI system in which personal data are processed, a data protection impact assessment in accordance with Article 35 GDPR will generally be required.

7. AI requires technical and organizational standards

In order to ensure processing in accordance with data protection regulations, technical and organisational measures pursuant to Article 24 and Article 25 GDPR, such as pseudonymisation, must be taken during design and usage of AI systems. This is not achieved solely by the assumption that the individual person will disappear in large amounts of data. As of now, no specific standards or detailed requirements for technical and organisational measures for a data protection compliant use of AI systems exist. Increasing knowledge in this area and developing examples of best practices is an important task for commerce, industry and science. The data protection supervisory authorities will actively accompany this process.

III. AI development requires regulation

The data protection supervisory authorities monitor the application of data protection law, they enforce it and they are to advocate effective protection of fundamental rights in further development of these laws. In view of the high dynamics in the development of AI technologies and the various fields of application, the limits of this development may not yet be foreseen. Similarly, the risks of the processing of personal data in AI systems cannot be rated in a general way. Ethical principles must also be observed. Apart from the scientific community, data protection supervisory authorities and users it is, especially, the political players who are required to accompany and to direct the development of AI in favour of the protection of personal data.

Discriminating tendencies are not always apparent from the outset. Therefore, an assessment of risks for the rights and freedoms of people has to aim at a reliable elimination of hidden discriminations through countermeasures before an AI system is used. Appropriate risk monitoring must be carried out also during the application of AI systems.

A further focus of the DSK's work involves the digitalisation of healthcare. The processing of health data entails particular risks, and so the DSK is calling for state-of-the-art protection of patient data, regardless of the size of the medical establishment processing said data. In particular, health-related websites and apps must meet expectations in respect

of confidentiality and comply with certain requirements when transferring personal data.

Accreditation of supervisory bodies for the monitoring of codes of conduct

Pursuant to Article 57(1)(p) GDPR, every supervisory authority must on its territory draft and publish the

criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41. Codes of conduct “clarify” the application of the GDPR. Clarification of this kind is necessary because the GDPR is often somewhat vague, and contains blanket clauses. Codes of conduct can be used as interpretation aids and therefore increase legal certainty. They do not serve as a legal basis for the processing of personal data, but they are a key facilitating tool – particularly in certain industries – for implementing the GDPR’s rules, some of which are highly abstract.

I was involved in drafting the European “Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation (EU) 2016/679” (see No. 3.2), the aim of which is to provide practical tips and guidance on the interpretation and application of Articles 40 and 41 GDPR, and to outline the rules and procedures for submitting, approving and publishing codes of conduct at national and European level.

One of the requirements laid down in the Guidelines is that a code of conduct should identify an accredited monitoring body (public bodies and authorities are exempt from this requirement). The task of this monitoring body is to carry out controls (alongside the competent data protection supervisory authority) to ensure that the code members are complying with the code’s provisions.

Germany’s criteria for accreditation of code monitoring bodies were forwarded to the EDPB for approval in keeping with the consistency mechanism pursuant to Article 64(1) sentence 2(c) GDPR.

Other topics

Other areas of work by the DSK included an investigation into the privacy-compliant use of Windows 10 (see No. 8.12) and the adoption of a report on experience gained in the implementation of the GDPR. The DSK’s aim in publishing this report was to contribute the practical experience of GDPR application gained by the German supervisory authorities since its entry into force to the evaluation process required in accordance with Article 97 GDPR. Following on from this, the DSK also wished to make suggestions for improvements with a view to making the GDPR easier to implement in practice.

The papers published by the DSK can be accessed at the following links:

<https://www.bfdi.bund.de/entschlueßungen>
<https://www.bfdi.bund.de/beschluesse->

[positions-papiere](https://www.bfdi.bund.de/kurzpapiere)
<https://www.bfdi.bund.de/kurzpapiere>

DSK Working Groups

Working Group on Tax Administration

Since 25 May 2018, I have been responsible for overseeing not only the Federal revenue authorities, but also the revenue authorities of the Länder covered by the scope of the [German] Fiscal Code (Abgabenordnung, AO). Pursuant to Section 32h AO, all revenue authorities within Germany that perform tasks pursuant to the Fiscal Code are therefore now under my oversight, and are no longer the responsibility of the data protection supervisory authorities of the Länder. I am furthermore responsible for overseeing the municipal tax offices in so far as these latter are responsible for handling property and business taxes.

As a logical next step, this change in the rules on jurisdiction has now been followed up by the appointment of a new chair for the Working Group on Tax Administration, which continues to be an important forum for clarifying any points that require coordination between the BfDI and the data protection supervisory authorities of the Länder.

Working Group on Principles

I am responsible for chairing the Working Group on Principles, which meets twice each year and whose members include representatives of all the data protection commissioners of the Länder. The substance of its work includes investigating questions of principle relating to data protection and drafting corresponding positions for presentation to the DSK.

Over the course of the past year, the Working Group on Principles carried out an in-depth examination into experiences of applying the GDPR. The report by the independent data protection supervisory authorities of the Federal Government and the Länder on experiences gained in the implementation of the GDPR was drafted by a sub-working group set up especially for this purpose and finalised by the Working Group on Principles (see No. 4.1). In addition, cooperation and collaboration was stepped up with the specific supervisory authorities established under Articles 85 and 91 GPDR, with a view to ensuring that Section 18 (1), fourth sentence, BDSG can be implemented appropriately.

The Working Group on Principles also investigated various individual questions of principle relating to implementation of the obligations to provide information pursuant to Article 13 GDPR and the right of access by data subjects pursuant to Article 15 GDPR, as well as a number of issues relating to joint controllers pursuant to Article 26 GDPR and processors pursuant to Article 28 GDPR.

[I recommend complying with the seven data protection requirements set out in the “Hambach Declaration on Artificial Intelligence” when implementing AI in a wide range of fields.](#)

Cross-references:

3.2 European Data Protection Board (EDPB), 4.1 Evaluation of the GDPR, 4.2 Digitalisation in the healthcare sector, 4.4 Artificial intelligence, 4.5.1 Consent to research

3.2 European Data Protection Board (EDPB)

During the reporting period, the EDPB adopted further guidelines on the uniform application of the GDPR and stepped up cross-border cooperation between the European data protection authorities.

The EDPB was established by the GDPR, and its primary task is to ensure the consistent application of the GDPR throughout the EU. It adopts guidelines, recommendations and best practices to this end, and can take decisions in cross-border cases that are binding on the data protection supervisory authorities of the EU Member States.

Members of the EDPB include the heads of the data protection supervisory authorities of the Member States and the European Data Protection Supervisor. As the joint representative of all of Germany’s supervisory authorities, the BfDI represents Germany within the EDPB.

The EDPB’s work this year was focused on the development of guidelines within the meaning of Article 70 GDPR to ensure consistent application. The EDPB also approved opinions within the framework of the consistency mechanism pursuant to Article 64 GDPR and discussed topical issues relating to data protection policy at international and EU level.

Guidelines

The EDPB adopted several sets of guidelines during the reporting period, all of which underwent a process of public consultation, and I was involved as co-rapporteur in drafting many of them. The relevant guidelines were as follows:

→ **Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies**

These guidelines provide practical tips and guidance on the interpretation and application of Articles 40 and 41 GDPR, and outline the rules and procedures for submitting, approving and publishing codes of conduct at national and European level. One of the requirements laid down in the Guidelines is that a code of conduct should identify an accredited monitoring body (public bodies and authorities are exempt from this requirement). The task of this monitoring body is to carry out controls (alongside the competent data protection supervisory authority) to ensure that the code members are complying with the code’s provisions.

→ **Guidelines 2/2019 on the processing of personal data pursuant to Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**

The Guidelines set out the requirements and conditions that must be met before undertakings offering online services can cite “performance of a contract” as the legal basis for the processing of user data. Pursuant to Article 6(1)(b) GDPR, the processing of personal data shall be lawful if and to the extent that said processing is necessary for the performance of a contract. The Guidelines clarify that the decision as to whether processing is necessary for the performance of a contract does not depend solely on the arrangements made in the contract. Instead, an evaluative decision must be carried out with regard to the data protection principles laid down in Article 5 GDPR (data minimisation, fairness, transparency). This means that, for example, “performance of a contract” cannot, as a general rule, be cited as a legal basis for data processing operations carried out with a view to user-targeted online advertising.

→ **Guidelines 3/2019 on processing of personal data through video devices**

The Guidelines contain guidance on choosing a position for video systems and the length of time for which surveillance recordings should be retained, and address current technologies such

as biometric video surveillance. They clarify that biometric data that can be used for the purpose of permanently identifying a natural person qualify as particularly sensitive data and can therefore only be processed under strict conditions.

According to the Guidelines, any controller wishing to track individual data subjects using permanent biometric identification, for example in order to monitor their movements and shopping behaviour in a department store, would as a basic principle need to obtain the explicit consent of all data subjects.

→ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

These Guidelines contain advice for controllers on how to implement the provisions of Article 25 GDPR by means of appropriate technical and organisational measures and necessary safeguards in order to protect the rights and freedoms of data subjects in an effective manner.

→ Finally, the EDPB revised and adopted final versions of the following guidelines that had been adopted in 2018 and had undergone public consultation: Guidelines 1/2018 on certifications, Guidelines 3/2018 on the territorial scope of the GDPR and Guidelines 4/2018 on the accreditation of certification bodies (see No. 8.10).

Opinions within the framework of the consistency mechanism

The opinions adopted by the EDPB during the reporting procedure as consistency findings pursuant to Article 64 GDPR related to lists of processing operations subject to the requirement of a data protection impact assessment pursuant to Article 35(4) GDPR or exempt from such a requirement pursuant to Article 35(5) GDPR. Lists of this kind are presented by the national supervisory authorities and analysed by the Technology Expert Subgroup to ensure that the same requirements apply in terms of data protection impact assessments in all the Member States. The EDPB's opinions on individual lists contained suggestions for revisions by the relevant supervisory authorities. This ensures that the consistency mechanism promotes uniform application of the GDPR.

The EDPB also acted pursuant to Article 64 GDPR by issuing opinions approving the binding corporate rules (BCR) of the UK company Equinix Inc. and approving the standard contractual clauses for contract data processing pursuant to Article 28(8) GDPR submitted by the Danish supervisory authority.

Additional consistency findings under Article 64 GDPR

concerned the interplay between the GDPR and the ePrivacy Directive and an administrative arrangement for the transfer of personal data between European Economic Area (EEA) financial supervisory authorities and non-EEA financial supervisory authorities.

Other work by the EDPB

As well as adopting general guidelines and opinions under the consistency mechanism, the EDPB examined and adopted opinions and reports on a number of different topics in the field of data protection policy. These included the legislative process for the ePrivacy Regulation and the consequences of Brexit for transfers of data from the EU to the United Kingdom in the event of a no-deal Brexit; guidance on this topic was also published for undertakings (see No. 8.1.1).

A further focus of the EDPB's work relates to data protection in the field of security. Together with the European Data Protection Supervisor (EDPS), the EDPB drafted an opinion on the US CLOUD Act (see No. 6.1.1) and investigated the Privacy Shield (see No. 8.1.3).

The "Future of Supervision" was another item on the EDPB's agenda. This relates to coordinated data protection supervision by the EDPB and the national supervisory authorities of major European IT systems and agencies such as Eurojust, the Schengen Information System (SIS), the Visa Information System (VIS) and the Entry Exit Register (EES), and the EDPB established a Coordinated Supervision Committee (CSC) for this purpose.

The topic of interoperability was also discussed. In a letter to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), the EDPB criticised the introduction of the Interoperability Framework aimed at the technical interconnection of a large number of EU databases in the field of justice and home affairs. The EDPB's specialist activities in the field of security are carried out by the Borders, Travel and Law Enforcement (BTLE) Expert Subgroup; I act as a coordinator and co-rapporteur of this Expert Subgroup, as well as a member of the Privacy Shield Monitoring Team.

A further key aspect of the EDPB's work relates to cooperation between supervisory authorities on cross-border data protection cases. The authorities exchange pertinent information and carry out joint assessments under the consistency mechanism pursuant to Article 60 GDPR in this connection. In my opinion, it is vitally important to ensure that supervisory authorities follow a uniform approach, particularly when dealing with data breaches by the

global tech giants that process and evaluate huge volumes of data.

The EDPB has not yet exhausted its full **potential for action** in this area. By the end of 2019, there was not a single major cross-border case relating to these companies in which a proposal for a decision by the competent national supervisory authority had been adopted.

Cross-references:

6.1.1 CLOUD Act, 8.1.1 Third-country transfers and 8.1.3 Developments relating to the EU-US Privacy Shield

3.3 Data protection committee of the Council of Europe

The Consultative Committee set up pursuant to Article 18 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) carries out important work on topics relating to data protection that fall under the jurisdiction of the Council of Europe. Given the extensive size of the Committee and the large number of parties to Convention 108, its work is hugely significant for citizens both inside and outside Europe.

Following the successful conclusion of negotiations on a Protocol amending and modernising Convention 108 of the Council of Europe, which was originally adopted in 1981 as the first legally binding international instrument in the field of data protection, October 2018 saw the launch of the process for signature and ratification of the Protocol by the current contracting parties to Convention 108. I am delighted to report that Germany was one of the first countries to sign this Protocol, and I hope that the domestic ratification process still ongoing within Germany can be completed promptly. Prompt ratification by the majority of the current parties to the Convention is important because a minimum quorum of signatory states must be achieved before the Protocol amending the Convention can enter into force. Only then can the new and more in-depth data protection principles of the modernised Convention 108 – frequently referred to as “Convention 108+” – come into effect.

Article 18 of the original version of Convention 108 provided for the setting up of a “Consultative Committee”, which has the following tasks pursuant to Article 19 of the Convention:

- make proposals with a view to facilitating or improving the application of Convention 108;

- make proposals for amendment of Convention 108;
- formulate its opinion on any proposal for amendment (by the contracting parties) of Convention 108;
- at the request of a contracting party, express an opinion on any question concerning the application of Convention 108.

Each contracting party is represented within the Consultative Committee. Following the establishment of the BfDI as an independent supreme federal authority, I attend the meetings of the Consultative Committee as an observer and am involved in its activities, alongside representatives of the German Federal Ministry of the Interior, Building and Community (*Bundesministerium des Innern, für Bau und Heimat*, BMI). The Consultative Committee has adopted many key recommendations and guidelines over the years, particularly in respect of the first of the tasks listed above. During the 2019 reporting period, topics examined by the Committee included profiling, facial recognition and data protection in the education system. Looking ahead to Convention 108+, it also began to lay the groundwork for a new task, namely evaluating – for the first time in the case of a new contracting party and at regular intervals in the case of existing signatory states – whether the level of personal data protection a country provides is in compliance with the provisions of the Convention.

Convention 108 of the Council of Europe is also noteworthy because of its global reach: in addition to the 47 Member States of the Council of Europe, including all the EU Member States and a number of other countries such as the Russian Federation, Turkey, Switzerland and Norway, an increasing number of non-European countries have ratified Convention 108 and, in some cases, also the Protocol amending and modernising the Convention; these currently include the Cape Verde Islands, Mauritius, Mexico, Senegal, Tunisia and Uruguay as well as Argentina and Morocco, which acceded to Convention 108 during the 2019 reporting period. The Council of Europe has received applications for accession from Burkina Faso and other countries.

3.4 International Conference of Data Protection and Privacy Commissioners

In 2019, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) studied the intersections between data protection supervision and other regulatory agencies, e.g. in the

fields of consumer protection and competition. It also launched a new name: “Global Privacy Assembly”.

The theme of the 41st ICDPPC in Tirana, Albania, was “Convergence and Connectivity: Raising Global Data Protection Standards in the Digital Age”; conference-goers debated the issue of whether the legislative areas of data protection, consumer protection and competition defence are converging or even overlapping. Discussions were also held on the extent to which the data protection supervisory authorities could pool their efforts with the regulatory authorities, to the mutual benefit of both parties. As an example of cooperation of this kind, I took part in a panel discussion during which I outlined the Facebook decision adopted by the German Federal Cartel Office in February 2019, and explained why I continue to believe it was appropriate, even though it has since been suspended by the Düsseldorf Higher Regional Court.

In terms of internal matters, the ICDPPC spent time thinking about its role going forward and adopted a programme of work for the years 2019 to 2021 (“Resolution on the Conference’s strategic direction”) with specific strategic priorities. A new “Policy Strategy Working Group” (PSWG) was set up as a steering group for this programme of work. A further goal pursued by the ICDPPC is to transform its discussion of topical and globally relevant issues into an ongoing year-round process rather than an annual event, and a new permanent Working Group was therefore set up to investigate general or case-by-case cooperation between ICDPPC members. I am involved in the activities of both of these new working groups with a view to supporting the vital work carried out by the ICDPPC in these areas. Work will also continue within the Working Group on the Future of the

Conference and the Working Group on Ethics and Data Protection in Artificial Intelligence.

The ICDPPC furthermore adopted a decision that will have major implications in terms of its public image: it will henceforth be known under the shorter and catchier title of “Global Privacy Assembly” (GPA). This name – which became the organisation’s official moniker on 15 November 2019 – also better expresses its status as a permanent association of data protection supervisory authorities from all over the world. Documents adopted by both the ICDPPC and the GPA can now be found on the website <https://globalprivacyassembly.org>.

Other work carried out by the 41st ICDPPC included the adoption of a number of resolutions; one related to the rapid removal of certain content from social networks, such as posts condoning terrorist or extremist violence, with the content posted by the perpetrator of the terrorist attacks in Christchurch (New Zealand) cited as an example. Another vitally important resolution concerned the relationship between data protection on the one hand and other fundamental rights and the functioning of democratic processes on the other, and potential interactions in this respect. Its purpose is to lay the groundwork for further resolutions to be adopted by the GPA in future on specific individual fundamental rights or processes, for example a citizen’s right to vote freely and without undue influence.

The resolutions adopted by the ICDPPC or GPA can be downloaded in English from my website (www.bfdi.bund.de/gpa); working translations of these resolutions into German are also available there.

4. Main Topics

4.1 Evaluation of the GDPR

The GDPR had been in force for over 18 months by the end of the reporting period for this activity report, which means that controllers, contract processors, data subjects (in relation to their rights) and – last but not least – data protection supervisory authorities are now able or obliged to apply its provisions in practice. Starting as early as May 2019, a significant number of events (conferences, panel discussions and talks, some of which were open to the public) were organised as initial stock-taking exercises. Looking ahead to the evaluation pursuant to Article 97 GDPR (to be carried out by the European Commission before the deadline of 25 May 2020), the independent supervisory authorities of the Federal Government and the Länder drafted a report on experience gained in implementation of the GDPR, and I played an important role in this process.

Notwithstanding a number of teething problems – which are unavoidable when rolling out new legislation on this scale (see No. 1.1 of the 27th Activity Report) – and the alarmist reporting by certain quarters, some of which was absurd, it is safe to say that several of the key goals pursued through the reform of European data protection legislation have been achieved. The fundamental right to informational self-determination is now better protected as a result of the far-reaching harmonisation of data protection legislation within the EU – aimed at eliminating obstacles to the digital internal market – and the rise in awareness of data protection issues among companies, authorities and citizens. Other contributing factors include the harsher sanctioning powers granted to the supervisory authorities, which are increasingly making use of these powers by imposing fines. The GDPR is regarded as a model or an inspiration for national data protection legislation in countries

such as the USA, South Korea, Mexico, Brazil and India, and has therefore contributed to a significant improvement in data protection practice not only in Germany and Europe, but all around the world.

My overall assessment of GDPR-related developments is therefore positive, but I believe that there is still room for improvement. Data protection enforcement continues to be a major sticking point, particularly with regard to the global IT giants. It is the responsibility of all European supervisory authorities to engage wholeheartedly in cooperation under the auspices of the EDPB so that the pressure brought to bear on these companies is sufficient to force them to comply with the requirements. Turning to other matters, it is also necessary to respond to the concerns and criticisms that have been voiced about the GDPR, and to discuss them at European level within the framework of the forthcoming evaluation process. Efforts should be made at the same time to eliminate unnecessary red tape, e.g. in relation to obligations to provide information and keep documentation, and to minimise existing loopholes in data protection law, for example as regards profiling.

DSK's Report on Experience Gained in Implementation of the GDPR

Pursuant to Article 97(1) GDPR, the European Commission must submit a report on the evaluation and review of the GDPR to the European Parliament and to the Council by a deadline of 25 May 2020. Pursuant to Article 97(3) GDPR, the Commission may request information for this purpose, inter alia from the supervisory authorities. This prompted the DSK to draft a Report on Experience Gained in Implementation of the GDPR and forward it to the EDPB, which is consulted by the Commission pursuant to Article 97(3) GDPR. The report was also published on the website of the DSK. The content of

the report centred around the following nine key topics:

- making life easier and practicability,
- notifications of personal data breaches,
- purpose limitation,
- data protection by design,
- powers of the supervisory authorities and sanctioning practice,
- competence, cooperation and consistency,
- direct marketing,
- profiling,
- accreditation.

Although the overall conclusion drawn by the DKS about the implementation of the GDPR is a positive one, it believes that improvements are required in these areas, and puts forward suggestions (or specific proposals) for legislative amendments. For example, it calls for the principle of “data protection by design” to be broadened in scope to cover product manufacturers and for the current legal framework on profiling to be tightened up in order to be able to set effective and enforceable limits to the use of personal data for the purposes of profiling. As regards making life easier and practicability in connection with the GDPR, the DSK proposes that, under certain circumstances, the obligations to provide information pursuant to Article 13 GDPR should apply only if the information is requested by the data subject. This would be the case if the data processing operations being carried out were such as could be typically expected under the specific circumstances.

In connection with the evaluation of the GDPR, I recommend backing the position of the national data protection supervisory authorities and the EDPB. This is particularly true in respect of the calls for meaningful steps to reduce the burden of red tape on small and medium-sized enterprises and for a tightening up of the legal framework for profiling.

4.2 Digitalisation in the healthcare sector

Digitalisation of the German healthcare sector holds many potential benefits for patients,

medical science, the care sector, funding agencies and society as a whole. At the same time, however, it involves the processing of large volumes of sensitive health data, and therefore requires a high level of data protection and data security in order to succeed. Patients must retain control of their own data, and it is also vital to ensure, at all times, that the ultimate outcome of digitalising health data is not the misuse of these data by private or state bodies or the stigmatisation or health profiling of individuals.

Digitalisation in the healthcare sector incorporates many different facets, such as the establishment of secure telematics infrastructure (see No. 4.2.1), improved communications between stakeholders in the healthcare sector, expanded opportunities for collecting and evaluating data, telemedicine, and support for medical treatments based on digital products.

After many years of delays, a great deal of money and effort is currently being channelled into digitalisation of the German healthcare sector. The [German] Act to Improve Healthcare Provision through Digitalisation and Innovation (*Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation*, DVG, see No. 5.6), one of the goals of which is to allow digital health apps to be prescribed by doctors and reimbursed by health insurance funds, represents one example of this phenomenon.

The healthcare sector faces major challenges in the field of data protection law; these take the form of issues such as the use of artificial intelligence and big data, the utilisation of cloud services for sensitive health data, the use of messenger services in hospitals and the unauthorised transfer of health data to third parties, such as tracking services. The recent scandals involving data protection in the healthcare sector illustrate how much harm can be suffered by a data subject who becomes identifiable and by society as a whole if sensitive personal health data or genetic data enter the public domain accidentally. It goes without saying that digitalisation of the healthcare sector will sometimes involve modifying long-established structures and adapting processes. At the same time, however, the right to informational self-determination should always take priority, and the risks should be minimised. The principles of data protection law – i.e. the principle that data should be collected only if it is necessary to do so, the principle that data should be retained only for a specific purpose, and the principle of data minimisation – should be observed at all times

rather than challenged by parties with their own interests.

Cross-references:

5.6 Legislation in the field of healthcare and social welfare

4.2.1 Telematics infrastructure and its applications

In the interests of secure communications in the healthcare sector, the Federal Government is working together with associations in this sector to create the necessary telematics infrastructure (TI). The first applications were rolled out during the reporting period, and plans were finalised for further applications such as the electronic health record. A number of problems were encountered in the process of connecting doctor's surgeries to the TI.

gematik GmbH is responsible for the security, interoperability, design and further development of the TI. Since 1 January 2019, service providers in the healthcare sector have been obliged by law to implement a system for the management of insured persons' master data as the first TI application (see Section 291 (2b) SGB Volume V).

In order to do so, they must purchase a connector certified for the relevant TI and connect their surgery's administrative system to the TI using this device. Since 1 July 2019, fees may be withdrawn from service providers that are not connected to the TI. This meant that there was an urgent need to clarify the question of which party should be regarded – within the meaning of the GDPR – as the controller for the TI under data protection law, and

I discussed this issue at length with my counterparts in the *Länder*. On 12 September 2019, the DSK found that gematik GmbH should be regarded as the joint controller for the TI under data protection law, since its guidance and specifications determine the purposes and means of processing data within the TI. The service providers should also be regarded as joint controllers, however, particularly as regards the operation of the connectors, since they are subject to certain due diligence obligations and will also use these connectors in the long term for secure transfers of patient data. The text of the resolution is reproduced in the box below.

A number of service providers have written to inform me that they have carried out a standardised "data protection impact assessment" regarding the installation of the necessary connector, and that they have decided – based on the outcomes of this assessment – they should not be regarded as controllers in respect of the connection of their surgeries to the TI. Yet if gematik GmbH can be regarded as the controller for the vast majority of the TI, it follows that the service providers cannot, and so they are not authorised to carry out a "data protection impact assessment" on the sections of the TI under gematik GmbH's responsibility.

Based on the BMG's current plans, one of the most important applications will be the roll-out of the electronic health record, which is scheduled for 1 January 2021. In my opinion, and assuming that insured parties will be able to opt for this record voluntarily and have full control over the use of the

Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany – Resolution of 12 September 2019

The DSK has reached the following conclusions regarding the identity of the controller under data protection law in respect of the telematics infrastructure pursuant to Section 291a (7) SGB Volume V:

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) is:

(a) the sole controller under data protection law for the central TI zone ("central TI platform zone"); and

(b) within the meaning of Article 26 GDPR, a joint controller under data protection law for the decentralised TI zone ("decentralised TI platform zone"). The scope of gematik's responsibility for the decentralised TI zone must be regulated by law. In particular, gematik is responsible for the processing of data if the parameters of this processing are determined by the specifications and configurations published by gematik in respect of the connectors, VPN access services and card terminals.

data stored in it, priority must be given to the implementation of a differentiated system for the management of rights and roles, allowing insured parties to grant access to individual service providers on a document-by-document basis. During the reporting period, I stepped up my efforts to convince the BMG that a differentiated system for the management of rights and roles should be implemented, and I will continue campaigning for such a system.

State-of-the-art systems offering the highest possible level of protection must also be put in place to prevent the electronic health record from being accessed by unauthorised parties. The electronic health card makes this possible, since access to a record can be gained only by someone in possession of the relevant card and the associated PIN.

The required level of security cannot currently be achieved by means of an alternative and legally permissible procedure for granting access, because the key material required for access would be stored in a location outside the data subject's control. Given that the unwanted disclosure of health data can have grave consequences, I advise against the use of an alternative access procedure unless it can provide the same level of security as the electronic health card. I have argued that the situation should be reviewed by 2022 at the latest to determine whether it might be possible to develop a viable alternative to a card-based access procedure, e.g. using "secure elements" in smartphones or tablets.

[I recommend that a differentiated system for the management of rights and roles should be implemented from the outset in connection with the electronic health record.](#)

4.2.2 Implant register

Two topics of increasing significance in the healthcare sector are the establishment of central registers and the use of these registers for research purposes. Goals pursued in this connection include the furthering of medical science and improved healthcare delivery, but these developments warrant close attention from the perspective of data protection law.

The BMG tabled 23 draft bills in the Bundestag over the course of the reporting year, which included the [German] Act on the establishment of an implant

register for Germany and other amendments to the Fifth Volume of the Social Code (*Gesetz zur Errichtung des Implantateregisters Deutschland und zu weiteren Änderungen des Fünften Buches Sozialgesetzbuch, EIRD*).

As a first stage, the specialist implant registers maintained to date by professional medical associations will be merged into a single implant register. The professional medical associations previously collected data from implant recipients on a voluntary basis, but the new implant register will be the first health register based on a mandatory and country-wide reporting obligation. It is significant from the viewpoint of data protection law for many reasons, the first of which being that the collection of data is based on a legal obligation rather than on voluntarily granted consent. Data subjects will also be unable to exercise their right to obtain restriction of processing pursuant to Article 18 GDPR or to object pursuant to Article 21. This is particularly controversial since the register – contrary to what its name might suggest – is not a register of products, but a compilation of large amounts of particularly sensitive health data, such as clinical and temporal data on the treatment process, including in particular anamnestic data, diagnostic findings relevant to the implant, indications, previous surgeries and weight. These data are stored in the register under a pseudonym previously assigned by a trust centre.

The BMG states that the purpose of the Act is to guarantee the safety of medical devices, safeguard the quality of implant-based healthcare and carry out market surveillance (vigilance). For example, the retention of pseudonymised data makes it possible to issue warnings about device defects to patients that may be affected. Various bodies will also be provided with the opportunity to carry out scientific research using these data.

During the consultations, I was able to make heard my opinion that the status of trust centre should be duly assigned to an institution operating independently of any registry authority or administrative office. I also expressed my concerns – during departmental discussions on the draft bill – about the fact that data subjects would be prevented from exercising all their rights under data protection law, but the most I could achieve in this respect was the restoration of certain rights that had originally been excluded, including the right of access pursuant to Article 15 GDPR and the right to rectification pursuant to Article 16 GDPR.

In so far as possible, the data made available for research purposes will be anonymised; in other words, they will generally consist of consolidated (aggregate) data concerning multiple individuals. Special requirements have been imposed on the provision of pseudonymised data. Once the register becomes operational, I will monitor whether the procedure for checking compliance with these requirements is being followed properly, and in particular how the administrative office in charge assesses whether a particular research project meets the relevant criteria in terms of needing to access the data. It was initially planned that the register would be operated within the German Institute of Medical Documentation and Information (*Deutsches Institut für Medizinische Dokumentation und Information*, DIMDI), and I regarded this as a wise choice. Yet the BMG's plans to integrate DIMDI into the Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte*, BfArM) have given rise to a new problem: how can a neutral procedure for deciding on applications to access register data be implemented if the BfArM itself is named in the Act as an authorised user and would therefore need to adjudicate on its own applications? Given the highly sensitive nature of the data involved, I made urgent calls for the tasks involved in operating the register to be assigned to an independent body so that they could be performed in accordance with data protection requirements.

The same is also true in respect of other registers in the healthcare sector. The BMG has postponed the merger of the DIMDI with the BfArM for the meantime, pending clarification of this issue.

[Instead of moving registers to the BfArM, I recommend creating a separate and independent registry authority for the healthcare sector.](#)

Cross-reference:

5.6 Legislation in the field of healthcare and social welfare

4.3 Data minimization

The principle of data minimisation is a perennial issue in the field of data protection law, and last year I once again received many complaints on this topic.

Data minimisation is one of the basic principles of European data protection law enshrined in Article 5 GDPR. The processing of personal data must be appropriate to the purpose and limited to what is

necessary. Controllers are therefore subject to an ongoing obligation to consider carefully which data are actually necessary to perform a particular task, and for how long they need to be processed.

The following examples illustrate the real-life implications of this principle for the work carried out by authorities.

Income tax assessment notices as a basis for calculating statutory health insurance premiums

The health insurance funds are obliged to collect certain data for the purpose of calculating premiums or checking exemptions from additional contributions. Individuals are asked to submit income tax assessment notices firstly if they are self-funding parties under a statutory health insurance fund, and secondly if they are insured via a family member with a whole-family policy.

Since the collection of data to calculate the level of employer premiums is unnecessary in the case of self-funding parties, the health insurance funds are obliged to collect these data via a different route. Under the social administration procedure, the authority may – at its discretion – use any evidence that it deems necessary to ascertain the facts of the case (Section 21 SGB Volume X).

With a view to ensuring that premiums are calculated uniformly, the legislator tasked the National Association of Statutory Health Insurance Funds (*Spitzenverband Bund der Krankenkassen*, GKV-Spitzenverband) with regulating the calculation of premiums. Documents published by the National Association of Statutory Health Insurance Funds for this purpose include the “Uniform principles governing the calculation of premiums by voluntary members of the statutory health insurance fund [...] (Procedural principles governing premiums by self-funding parties)”, which – supplemented by the list of revenue types and their assessment under the law of contributions pursuant to Section 240 SGB Volume V – specify the types of revenues covered by the term “income”.

These principles also stipulate that the health insurance funds must collect the necessary documentary evidence on an annual basis. The income of a spouse or cohabiting partner is relevant only if the latter has no statutory health insurance. Nevertheless, this information may be used to determine whether a whole-family insurance policy is held.

An income tax assessment notice is an official document that can fulfil its legal evidentiary function only if it is presented in full. Pursuant to Section 157 AO, the mandatory components of a tax assessment notice include details of the assessed tax (type and amount), instructions on applicable legal remedies and details of the authority issuing the notice. While observing these requirements, any data in an income tax assessment notice that are not required for the purpose of determining income as a basis for premium calculations should be redacted.

I believe that consideration should also be given to other, more privacy-friendly solutions. For example, insured parties could produce a personal declaration covering the portion of their income that is relevant in terms of premiums, ask the tax authorities to certify the declaration, and then forward it directly (via electronic channels) to the competent health insurance fund upon request.

Collection of data by job centres from self-employed benefit recipients

Recipients of subsistence benefits under Volume II of the Social Code include many self-employed persons whose income is not high enough to cover the costs of living. It can be particularly challenging to determine whether these individuals are entitled to receive benefits, since all revenues from self-employed activities must be taken into account and offset against the associated essential expenses. Job centres are often obliged to request comprehensive information and documentation. Yet it is frequently the case that the job centres do not require certain types of data (in particular personal data) belonging to benefit recipients in order to perform their tasks, since individual revenue and expense figures can be assigned to invoice numbers, or some other suitable system can be used. The job centres must therefore inform benefit recipients that they are entitled to have their personal data redacted; this will ensure that these centres do not obtain personal data that they do not require for the performance of their statutory tasks.

Submission of pension statements to the job centre

Subsistence benefits under Volume II of the Social Code are paid only if the individuals in question are not entitled to higher-ranking social security benefits. These individuals must therefore submit a

pension claim if their entitlement to a retirement pension is high enough and they are approaching retirement age.

However, job centres may ask these individuals to submit a pension claim only if receipt of the retirement pension would eliminate all need for welfare assistance, i.e. they would no longer be dependent on benefits to cover the cost of living. To determine whether this is the case, job centres frequently need to request full pension statements.

In the event that the individual in question is entitled to only a very small retirement pension, however, a partial pension statement may suffice. If the pension forecasts on this statement prove that the entitlement will fall a long way short of eliminating the need for welfare assistance, the requirements for the mandatory submission of a pension statement are not met, and no further evidence will be required in this instance.

If the level of entitlement renders it possible that receipt of the pension might eliminate the need for welfare assistance, an up-to-date pension statement must be presented for the purpose of determining the exact date on which early retirement would be possible and the pension that would be paid upon early retirement. There is no obligation to request a comprehensive pension statement, however. The list of pension periods and the breakdown of earning points bear no relevance to the performance of tasks by the job centres.

Requests by job centres for proof of tenancy

I described in my 24th and 26th Activity Reports how recipients of benefits under Volume II of the Social Code were being asked (with reference to their duty to cooperate) to present certificates with proof of their tenancy agreement, filled out by their landlords. I regret to say that this procedure is still in place at certain job centres.

Certificates supplying proof of tenancy agreements can be used only on a voluntary basis. They are a straightforward means of providing all the evidence required to check whether the individual in question is entitled to housing and heating benefits. At the same time, however, this form of evidence can be used only by individuals with landlords who are already aware that their tenants receive benefits or who do not object to renting their property to benefit recipients.

Yet many people who are in receipt of benefits are reluctant to disclose this fact to their landlords. In most cases, it is possible to circumvent the problem by requesting other documents that contain the information required to calculate an entitlement to housing and heating benefits, for example the rental agreement, utility and service charge bills and account statements. Job centres must ensure that they do not create an artificial need for data processing in the course of their work, for example a disclosure to landlords that their tenants are receiving benefits.

Publication of trade mark applicants' personal data

In accordance with the provisions of the [German] Trade Mark Act (Markengesetz, MarkenG) and the [German] Trade Mark Regulation (Markenverordnung, MarkenV), the German Patent and Trade Mark Office (Deutsches Patent- und Markenamt, DPMA) publishes trade mark applicants' personal data in its online register. At first glance, there appear to be valid reasons for doing so. For example, the holders of rights to existing trade marks must be able to engage in discussions with a party applying for a new trade mark if said trade mark might give rise to a risk of confusion.

Yet the DPMA continues to provide public access to applicants' data even if a trade mark application fails (which may happen for many different reasons), even though from that point onwards there is no longer any need for third parties to engage in discussions with the applicant. The DPMA claims that it publishes these data for the purpose of providing the public with some insight into its decision-making processes, yet the same goal could also be achieved by publishing failed trade mark applications without the applicants' personal data.

When I informed the German Federal Ministry of Justice and Consumer Protection (Bundesministerium der Justiz und für Verbraucherschutz, BMJV) that I intended to exercise my powers under Article 58(2) GDPR against the DPMA, the BMJV concurred with my interpretation of the law. The DPMA was asked to make changes to the procedure I had criticised, and to remove applicants' personal data from its online register in the event that their trade mark applications failed. The DPMA was also asked to introduce a procedure for erasing the data relating

to an application at the point when there ceases to be a requirement for their continued storage. Work is currently in progress on the necessary technical modifications, which are expected to be completed before the end of 2020.

4.4 Artificial intelligence

Artificial intelligence is currently one of the hottest topics in the field of technology, and rightly so. It is a linchpin technology that is fundamentally altering our economy and society at a number of different levels, and this process has already been ongoing for some time.

AI can assist us in many areas of life. It helps doctors to make better diagnoses and try new treatment methods, it helps organisations such as public transport companies to optimise resource deployment, and it helps us all to use energy more efficiently and reduce power consumption. These few examples should provide some indication of the vast range of opportunities opened up to us by AI.

“A particular concern of AI is to design “technical systems” in such a way that they can deal with problems themselves by adjusting autonomously to changing conditions. These systems are characterised by the fact that they are not programmed in the traditional manner; instead, they “learn” from new data and can handle uncertainties.”

Interpretation of the Federal Government, *Bundesrat* Printed Paper 19/1982

Our challenge: balancing the opportunities and the risks

These manifold opportunities are equally obvious to those of us working in the field of data protection, and we ourselves have considered how AI might be used to help us monitor data processing operations. As a general rule, however, greater opportunities mean greater (and new) risks. AI calls for large volumes of data, and these data are frequently personal in nature. For example, insurance companies might offer new incentive-based premium models using AI systems, perhaps with a view to promoting healthy habits. Yet those same citizens who are initially happy to benefit from cheap insurance premiums may quickly

become aware of the ambiguous nature of modern AI data analysis methods when the fully automated system sends them a higher bill for premiums – or perhaps even tells them that they are no longer eligible for coverage – because they have made changes to their lifestyle or learned of a predisposition to a certain medical condition.

Goal: proactive technology design

I intend to remain actively involved in efforts to encourage positive technology design in the field of AI. It is vitally important that human dignity and the associated fundamental right to informational self-determination should remain the benchmarks for our actions when using AI systems. Humans must not be degraded into simple objects, and data protection can help to promote this “human-centred” approach to designing AI systems. After all, data protection law contains many different normative provisions regulating fundamental ethical issues. Giving a platform to those who work in the field of data protection is therefore an essential factor in the ethical design of AI systems that are compatible with fundamental rights.

Data protection as a success factor

Data protection can be regarded as a vital key to success in this area, and we would be well advised – not least from the perspective of industrial policy – to place even greater emphasis on ensuring that Europe’s AI solutions comply with data protection requirements. The role of data protection is often misunderstood in this connection, however; it does not seek to restrict or impede innovation, but to strike a balance between the interests of third parties wishing to use data and the sovereignty of the individual. The overall aim must be to allow individuals to determine their own privacy preferences, while at the same time making full use of the opportunities afforded to us by digitalisation. Protecting privacy is an important task for many reasons, not least because it guarantees a space for individuals to engage in self-development without being subject to constant surveillance. Privacy-friendly AI could grow into a positive differentiator on a global market, and key strategic decisions will be taken in this area over the next few years.

Hambach Declaration – our initial position paper

“AI and data protection” was also one of the central topics examined by the DSK in 2019, and this organisation presented an initial position paper on

the privacy-friendly design of AI back in early April 2019, known as the Hambach Declaration (see box in No. 3.1). Alluding deliberately to the demands for freedom and democracy made at the Hambach Festival in 1832, the DSK emphasised that the use of artificial intelligence must be accountable to human beings and their fundamental rights and freedoms.

The following data protection requirements were identified in the Hambach Declaration:

- AI must not turn human beings into objects.
- AI may only be used for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation.
- AI must be transparent, comprehensible and explainable.
- AI must avoid discrimination.
- The principle of data minimisation applies to AI.
- AI needs responsibility.
- AI requires technical and organisational standards.

Practical recommendations for AI systems design in compliance with data protection requirements

The DSK built on the requirements set out in the Hambach Declaration by using them as a basis to develop practical recommendations for AI-specific technical and organisational measures. The “Recommendations for the design of AI systems in compliance with data protection requirements” were adopted in the form of a position paper on 6 November 2019 at the 98th Conference of the Independent Federal and State Data Protection Supervisory Authorities of Germany¹ and provide guidance for controllers on the aspects of data protection law that apply when planning and operating AI systems. The position paper is also intended to serve as a basis for a further stepping up of dialogue with the relevant stakeholders, such as the consumer associations.

Cross-sectoral dialogue as the only route to solutions that safeguard everyone’s interests

A great deal of my time over the past year was devoted to fostering this dialogue. For example, I organised a symposium under the heading “Chances and risks for the privacy-friendly use of

¹ The recommendations are available at <https://www.bfdi.bund.de/beschlusse-positionspapiere>

artificial intelligence”, held on 24 September 2019 in Berlin. The event served as a forum for discussion among over 150 attendees from a wide range of different disciplines, who exchanged views on the diverse, complex and, in some cases, contradictory interests of stakeholders in the field of AI. As a member of the DEK, I was able to highlight the enormously important role played by the fundamental principles of data protection law. Key requirements in this respect include not only transparency, but also effective algorithmic controls, and the DEK follows a risk-based regulatory approach in this area. The greater the potential for harm, the greater the need to apply stringent requirements to use of the algorithm, and the greater the need for opportunities to carry out controls. Further details of the DEK’s work can be found in No. 4.6 (Opinion of the Data Ethics Commission).

I am closely monitoring developments in respect of the Federal Government’s “Artificial Intelligence Strategy”, *inter alia* through my involvement in a Data Protection Round Table. It goes without saying that artificial intelligence does not respect borders, and I have therefore spoken out at EU and international level regarding the need for AI-related data protection concerns to be placed centre stage. My work within the ICDPCC’s Working Group on Ethics and Data Protection in Artificial Intelligence, which was set up in late 2018, represents a particular focus of my efforts in this respect.

Cross-reference:

4.6 Opinion of the Data Ethics Commission

4.5 Consent under data protection law

Consent is one of the key legal foundations for the processing of personal data. It should reflect a data subject’s intent as closely as possible, and is therefore the most direct basis for data processing. For this reason in particular, it is important that the requirements set out in law are observed consistently and strictly.

Article 6(1) sentence 1(a) GDPR allows the processing of personal data *inter alia* if the data subject has given consent to their processing. Yet the legal requirements that apply to consent are regulated not only in this Article, but also in Article 4(11) and Article 7(2) and (3) GDPR. According to these provisions, consent to a specific data processing operation must, in principle, be freely given, specific, informed and unambiguous.

The following two topics relating to consent are currently the subject of much debate.

4.5.1 Consent to research

The GDPR is designed to be compatible with research interests, but this does not mean that researchers enjoy complete freedom when it comes to processing personal data. The method of “practical concordance” must be applied as a means of striking an appropriate balance between the fundamental right to academic freedom and the fundamental right to data protection.

Article 89 GDPR stipulates that the GDPR applies to scientific research. Unless otherwise regulated by law, the processing of personal data for the purpose of research studies may therefore be lawful if consent is obtained from the data subjects. This consent must meet the requirements for informed consent within the meaning of Article 4(11) GDPR, i.e. data subjects must provide a “freely given, specific, informed and unambiguous indication of [their] wishes” by which they signify agreement to the making available of their data for a particular research study.

Recital 33 GDPR sets out a derogation from this principle by stating that “It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection.” Therefore, data subjects should be allowed, in narrowly constrained circumstances, to give their consent (“broad consent”) to:

1. certain areas of scientific research, or
2. parts of research projects,
3. when in keeping with recognised ethical standards for scientific research.

This derogation was welcomed by the research community, but the interpretations it allows are too broad.

In its decision of 3 April 2019, the DSK pointed out that, if consent is obtained in narrowly constrained circumstances a long time before data are collected, changes to the stated purpose of data processing can be tolerated only if the specific design of the research project renders it unlikely that the purpose will be apparent in full by the time when the data are collected. In this decision, the DSK makes it clear that a blanket broadening of purpose through the use of collected data for research in specific areas can no longer be deemed

compatible with the GDPR. It also points out that, “in the isolated cases in which it can be regarded as absolutely essential to obtain broad consent”, the necessary corrective measures should be taken to compensate for the fact that the purpose of the research is described in more abstract terms. These might include additional safeguards to promote transparency and build trust and additional data security guarantees.

Recital 33 GDPR refers to compliance with the “recognised ethical standards for scientific research” in connection with “broad consent”. These standards have included informed consent since the adoption of the Nuremberg Code in 1949, in part because of the medical experiments carried out under the Third Reich, but also in response to other ethically dubious research studies around the world. In an opinion published in 2017 and entitled “Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom”, the German Ethics Council (*Deutscher Ethikrat*) introduced the model of a “data donation”. This model should facilitate the individual’s ability to allow, by means of a comprehensive consent agreement, the use of their data, without strict earmarking, for the purposes of basic clinical and **medical research**. This would no longer qualify as informed consent within the meaning of Article 4(11) GDPR or “broad consent” within the meaning of recital 33 GDPR, but “blanket consent”, which is incompatible with the provisions of the GDPR.

During the reporting period, consent forms were nevertheless submitted to the data protection supervisory authorities of the Federal Government and the *Länder* that provided for a “data donation” of this kind. Thanks to our interventions, the consent forms were revised to bring them into line with data protection requirements.

As part of my work within the DEK, I was involved in the drafting of proposals on how tools such as dynamic consent or data custodians could be deployed to ensure that the use of data for medical research purposes complies with the principles of data protection.

4.5.2 Tracking and cookies

Many websites use tracking services. Cookie banners that presume consent if the user continues to the site are legally invalid, but a large number of website owners – including certain well-known ones – have not yet brought their websites into line with legal requirements.

Anyone who operates a website has an interest –

and in many cases a legitimate and comprehensible interest – in obtaining certain information, for example visitor numbers and details of click-throughs. This becomes problematic only if third-party providers are involved and data about users of the website are transferred to these providers. Consent from the user is required if the third-party providers wish to process these data further for their own purposes (e.g. Google Analytics with the standard configuration).

The cookie banners used on many websites for this purpose incorrectly lead the user to suppose that continuing to the website can be construed as consent. Consent must be informed and explicitly given, however. In other words, providers must first supply detailed information on the data that will be collected and the purposes for which they will be used. Only if users grant consent in return may the providers collect and process the data. Strategies such as pre-ticking boxes or hiding information in the small print (e.g. regarding the right to object) are not permitted.

At the same time, however, consent does not need to be obtained from users each and every time. I find it astonishing how many website owners plaster enormous cookie banners across their sites and respond to user complaints by stating that they are forced to do so by the GDPR or the supervisory authorities. This is quite simply not the case. No consent and no cookie banners are needed to collect visitor statistics in compliance with data protection law (provided that visitor statistics are all that is being collected). The DSK has described one possible approach in a detailed guidance document (available at: www.bfdi.bund.de/orientierungshilfen).

4.6 Opinion of the Data Ethics Commission

In its final opinion, the DEK emphasises the enormous significance of data protection and sets out specific recommendations as a basis for shaping our digital future. It is now up to the Federal Government and the Bundestag to follow up on these recommendations and take the appropriate steps.

On 18 July 2018, the DEK was tasked by the Federal Government with examining key questions clustered around three main topics: algorithm-based forecasting and decision-making, artificial intelligence and data. Its 16 members came from the fields of science, business, and consumer and data protection. Together with Ms. Marit Hansen,

Data Protection Commissioner of Land Schleswig-Holstein and Head of the Independent Centre for Privacy Protection Schleswig-Holstein, I represented the field of data protection.

An initial list of questions issued by the Federal Government served as the substantive framework for the DEK's work. According to the relevant document, its task was to "develop [...] guidelines for the protection of individuals, the preservation of social cohesion and the safeguarding and promotion of prosperity in the information age". It was furthermore tasked with providing recommendations on how these "ethical guidelines can be developed, respected, implemented and monitored".

The DEK could have spent many years debating the questions posed to it, but a deadline of one year was imposed by the Federal Government. After a great deal of hard work, the members of the DEK presented their final opinion to the Federal Government in October 2019. This opinion was adopted unanimously and without dissenting votes. In its opinion, the DEK not only emphasises the abstract importance of the individual's right to informational self-determination, but also provides specific recommendations for ways in which this self-determination can be integrated more effectively into the process of digital development.

Data and the protection of fundamental rights in a digital age

It was clear to me from the outset that robust data protection is a *sine qua non* for an ethical and fair data policy. This also reflects the position of the DEK, which has stated quite clearly that the framework for data protection should be tightened up. Statements of this kind counteract the erroneous belief that regulating as lightly as possible and doing away with existing statutory requirements wherever possible is a good idea as far as digitalisation is concerned. At the same time, however, regulation should not be a goal in and of itself. Its aim should be to safeguard the values of our legal system and to protect fundamental rights, and regulatory efforts should prioritise areas where the risks to legally protected rights are particularly pressing. For many decades, and since the 19th century at the very latest, every technological leap forward has been accompanied by the adoption of corresponding legislation, for example to protect the general public against specific risks. Examples include occupational health and safety regulations and rules governing motor vehicle design.

When we talk about regulating digitalisation, however, we are referring not only to informational self-determination and data protection. Given that digitalisation is gradually becoming an established part of every sphere of life, it is also having an impact on other legally protected rights, such as health, the freedom to engage in an occupation or the right to equal treatment. Examples that can be cited in this connection include AI in health research, personal care robots, automated recruitment procedures or the risk of discrimination as a result of poor or defective data sets.

The DEK therefore believes that regulation is necessary in areas where there is a risk to the legally protected rights of individuals or the general public. Examples include clearer regulations and greater transparency regarding profiling, a ban on algorithms with untenable potential for harm and specific rules on data trading.

Transparency

The topic of transparency is a leitmotif that occurs throughout the final opinion. From the perspective of data protection, transparency is a vital tool in our arsenal for dealing with increasing digitalisation. It will be possible for individuals to make use of their right to informational self-determination and to exercise the resulting data protection rights only if they have access to sufficient information. Informed consent can be obtained only from individuals who are aware of the nature of the personal data that will be collected, the purposes for which the data will be used and the third parties to whom the data will be transferred. The right of access, the right to rectification and the right to erasure can be exercised only by individuals who know which controllers are using their personal data.

The potential uses of data have become so complex and all-encompassing in recent years that it is often impossible for individuals to gain an overview of how their data are being used. Many people have stopped reading privacy notices and simply consent to everything. Others, particularly those belonging to the older generation, are afraid to participate in the digital society because they fear that their data will be misused. Neither of these two extremes is a desirable state of affairs. Instead, targeted transparency obligations should restore to citizens their right to digital self-determination in respect of personal data.

The DEK therefore set out a number of data ethics principles in its opinion, one of which relates to interest-oriented transparency: "Controllers must

be prepared and in a position to account for their data-related activities. This requires appropriate documentation and transparency and, if necessary, a corresponding liability regime in place.” This principle serves as a starting point for a number of recommendations for ways in which transparency could be strengthened, for example in the fields of profiling, scoring, icons for products and services, and the labelling of bots.

Profiling and scoring

I have called for more effective regulation and increased transparency in the area of profiling, and in particular scoring, for many years (see No. 5.3 of the 25th Activity Report). The DEK reiterated my demands, referring to “specific labelling, disclosure and information obligations” in respect of profiling as such. These information obligations should apply not only to automated decisions, but to the use of algorithms for profiling purposes in general. Similarly, the DEK calls for the right to a “digital new start” involving the erasure of existing profiles, e.g. upon reaching the age of majority.

Icons for products and services

The DEK endorses the adoption of binding provisions mandating the privacy-friendly design of products and services, particularly if these latter are targeted at consumers. In the same vein, the DEK has also called for the introduction of standardised icons that would allow consumers to make informed purchase decisions. For example, they could be used to inform consumers at a glance whether a device records personal data using sensors such as cameras or microphones, and whether these data are transferred to the manufacturer or even to third parties via the Internet.

Labelling of bots

The DEK has called for mandatory labelling of social bots. It believes that the authenticity of interpersonal communication is a fundamental condition for trustworthy interaction within society, and that social bots should therefore be labelled if there is any risk of confusion between human and machine. There is a particularly urgent need for a mandatory labelling scheme of this kind in the field of social networks and other intermediary platforms. Attempts are being made to exercise influence over the formation of public opinion through the use of social bots on these networks, and so there is a risk to democratic discourse. It should also be acknowledged that certain individuals (known as “trolls”) can also interfere in the formation of public opinion for

manipulative reasons, and that controversy exists over exactly how much influence bots wield.

Controls of algorithmic systems

Risk-based controls of algorithmic systems represent another key concern of the DEK. Public debate on the ethical implications of algorithms focuses heavily on the use of AI and machine learning, but the ethical issues that arise in connection with the use of algorithms apply just as much to standard or “traditional” algorithms as to AI (see No. 4.4 above for a further exploration of AI). In its recommendations, therefore, the DEK does not, as a general rule, differentiate between algorithms on the basis of their nature; instead, it refers to “algorithmic systems”.

As in other areas, the Data Ethics Commission has opted for a risk-adapted regulatory approach to the use of algorithmic systems. Future regulatory efforts should take an algorithmic system’s potential for harm as their starting point.

The DEK recommends developing a comprehensive model that can be used as a basis for assigning algorithmic systems to different levels of criticality (see illustration). The greater the potential for harm, the more stringent the requirements for use of the algorithm must be, and the more control options must be made available. The levels in this model range from applications with zero or negligible potential for harm (Level 1), in respect of which there are no special quality requirements or control mechanisms, through to applications with untenable potential for harm (Level 5), which should be completely or at least partially banned.

With a view to implementing a regulatory model, the DEK recommends that the Federal Government should push for an EU regulation on algorithmic systems enshrining horizontal requirements and setting out the central basic principles for algorithmic systems. It would be important to ensure that any such regulation included provisions on the admissibility and design of algorithmic systems, transparency and data subjects’ rights.

Innovative data management systems

The DEK’s recommendations are intended not only to highlight existing barriers to new digital products, but also to promote developments that promise to be particularly beneficial for individual citizens or the general public. It is therefore in favour of allocating funding to innovative data management and data trust schemes.

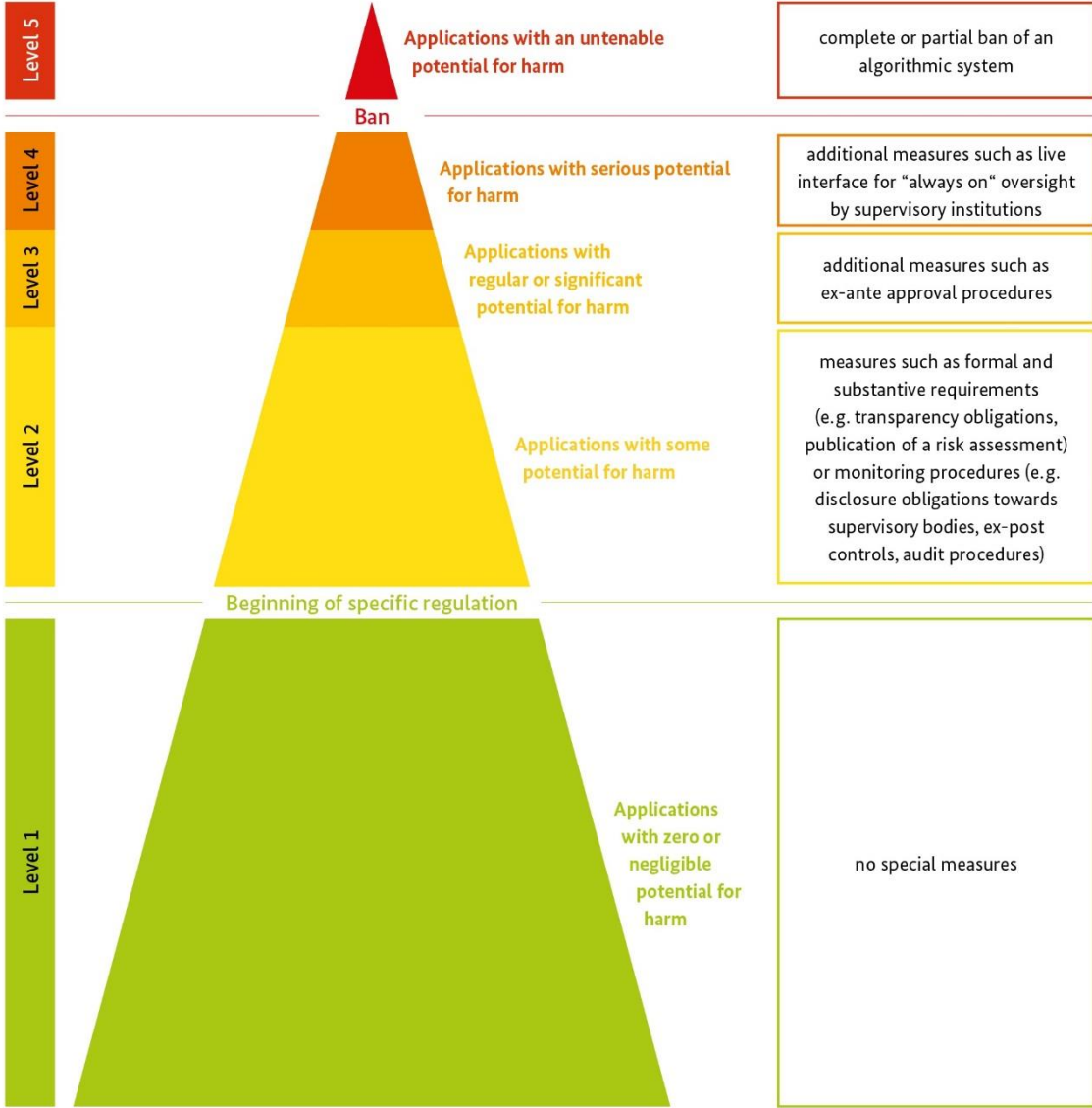
Digitalisation and data protection are not irreconcilable opposites. Instead, digital innovation

can make a vital contribution to strengthening data protection; examples include recent developments in the area of data management and data trust systems.

The terms “data management system” and “data trust system” refer to an extremely wide range of different models. Privacy management tools (PMT) range from applications that make consent management easier for users (dashboards, etc.) through to AI tools that automatically implement individual user preferences (“data agents”). Where the focus is not so much on the provision of technical applications and supporting these applications but rather on the service end, it is more common to use the term “personal information management systems (PIMS)”. Such services range through to offers (both comprehensive and less so) for third-party

management of user data (data trust models). The goal in both cases is to allow individuals to control their personal data. The DEK recommends that research and development in the field of data management and data trust schemes should be identified as a funding priority.

There is nevertheless a risk that the use of privacy management tools/personal information management systems might achieve the opposite to what is intended if they are not designed properly. Instead of facilitating genuine self-determination, privacy management tools/personal information management systems might also be used for external determination if an individual were careless or unaware. In the DEK’s opinion, there is therefore a need for further regulation to support the use of data management and data trust schemes. Quality standards and a certification and



monitoring system must be developed for privacy management tools/personal information management systems.

Cooperation between all the controllers involved is necessary to ensure that privacy management tools/personal information management systems can achieve sufficiently wide-ranging coverage. Controllers should therefore be obliged, under appropriate conditions, to ensure that access to data by the privacy management tools/personal information management systems can be monitored.

Provided that these requirements are met, privacy management tools/personal information management systems could serve as a key interface between data protection concerns and the data economy. In particular, they might facilitate the use of personal data for medical research.

Data anonymisation

The final opinion also addresses the issue of data anonymisation. In practice, it is often difficult to determine whether a data set consists of clearly personal, pseudonymised or anonymous data. Different legislative provisions apply in each case, and so it is vitally important for data controllers to know when they are working with personal data and when they are not.

The DEK has called for work to be stepped up on the development of data anonymisation procedures and standards. Workable anonymisation standards should be adopted at EU level with a view to achieving greater legal certainty. This might involve presumption rules that apply when the standards

are met. At the same time, however, it must still be possible for data protection authorities to rebut the presumption in case of need, if the standards are overtaken by technical reality and it becomes possible to link data to an individual again.

Other key topics covered in the opinion include the following:

- a proposal to introduce interoperability or interconnectivity obligations for providers in certain sectors (e.g. messenger services),
- a proposal to reassess liability law in view of the use of algorithms,
- a call to expand the scope of open government data (OGD) concepts,
- recommendations concerning access to data sets for researchers, and
- a call for improved protection of data by businesses.

A more detailed examination of these topics lies beyond the scope of this document; further information is available on my website, however. The opinion can be accessed via the following link: www.bfdi.bund.de/dek.

[I recommend that the proposals put forward by the Data Ethics Commission should be enshrined in law](#)

Cross-reference:

4.4 Artificial intelligence

5. Legislation

5.1 The Omnibus Act on the General Data Protection Regulation

The “Omnibus Act” amending over 150 different acts has now been adopted, meaning that the Federal Government’s sector-specific data protection regulations have also been brought into line with the provisions of EU law.

The GDPR has been directly applicable law in all of the EU’s Member States since 25 May 2018. Some of its provisions allow the national legislators a certain amount of regulatory flexibility, but others set specific regulatory tasks for the Member States. Further to one of these latter, Germany was obliged to review its sector-specific data protection legislation to ensure that it was compatible with the GDPR, and to amend it if necessary. The relevant amendments are contained in the Second Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (the “Omnibus Act”).

To guarantee smooth interactions between the GDPR and the Law Enforcement Directive on the one hand and German data protection legislation (which is highly differentiated) on the other, the first step taken was to replace the previous Federal Data Protection Act with a new version of the same Act, and to amend the key provisions of tax law and social data protection law already contained in the Fiscal Code and Volumes I and X of the Social Code to bring them into line with the provisions of the GDPR (see Nos. 1.2, 3.1.1 and 6.1.1 of the 27th Activity Report).

The Omnibus Act adapted a great many other provisions of the Federal Government’s existing sector-specific data protection legislation to bring them into line with the provisions of EU law. Over 150 acts were amended; comments on a number of these are set out below.

Federal Act on Registration

Alongside the necessary terminological changes, a number of substantive changes were made to the

[German] Federal Act on Registration (*Bundsmeldegesetz*). I put forward a great many proposals for changes of this kind as part of my involvement in this department’s work. For example, a data subject’s right of access was previously restricted by Section 10 of the Federal Act on Registration to cases in which data were transferred through automated retrieval or automated provision of information from population registers; this restriction has now been abolished. In future, the registration authorities must provide information upon request about all transfers of data from population registers. As a basic principle, therefore, citizens are entitled to comprehensive information regarding the data stored about them in the population register and regarding any recipients of these data. The option of providing information from population registers for the purposes of advertising or selling addresses has also been abolished. A further major substantive change relates to the release of additional information from the population register: Section 45 (2) of the Federal Act on Registration previously imposed an obligation on the registration authority to inform data subjects of any such release, but this obligation now lies with the recipient of the information pursuant to Article 14 GDPR.

Relaxation of the obligation to appoint data protection officers

I regret to say that the obligation to appoint data protection officers has been relaxed. Controllers and processors must now appoint a data protection officer only if at least 20 people (rather than 10, as was previously the case) are typically engaged in full-time tasks involving the automated processing of personal data. I made my position on this matter clear during the legislative procedure, as did the DSK. In return for a reasonable outlay on the part of the company, data protection officers provide expert advice on points of data protection law, thereby preventing data breaches before they happen and minimising the risk of sanctions. The system has been in place in Germany since the 1970s, and has proved particularly helpful when transitioning to the GDPR regime.

Lack of amendments to the Telecommunications Act

The Omnibus Act did not contain any amendments aimed at bringing the data protection provisions of the Telecommunications Act into line with the GDPR. Germany has not yet complied with its obligations under EU law in this area. Instead, the continued formal existence of the previous data protection provisions of the Telecommunications Act makes it difficult under certain circumstances to determine which provisions of data protection law (the provisions of the GDPR or the provisions of the Telecommunications Act) apply to certain cases under telecommunications law, and to determine the extent to which the Telecommunications Act is subject to the fundamental principle enshrining the primacy of application of the GDPR. This gives rise to significant legal uncertainty among data subjects (see No. 5.2).

Need for regulatory action in connection with the statutory health insurance funds

The regulator still needs to clarify the impact of consent in the relationship between insured parties on the one hand and the statutory health insurance funds on the other. Based on the numerous complaints I receive from insured parties, it is evident that there is a great deal of uncertainty about how to deal with situations in which insured parties are encouraged by health insurance funds (which have no legal footing to do so) to consent to the transfer of their medical data.

No agreement has been reached as to whether fines can be imposed in the event of data breaches by statutory health insurance funds. There is no plausible reason why the statutory health insurance funds, which increasingly view themselves as commercial enterprises, should be given preferential treatment in this area, and this is all the more true because the legislator has heightened the level of competition between the health insurance funds yet further by means of the Act for Fair Competition among Health Insurance Funds. If there is no way of imposing fines in the event of data breaches, data protection will not rank equally with other factors when carrying out a commercial assessment of processes within the statutory health insurance funds.

Cross-reference:

5.2. Further wait for amendments to the Telecommunications Act

5.2 Further wait for amendments to the Telecommunications Act

The primacy of application of the GDPR means that some of the data protection provisions that are still enshrined in telecommunications law – and still appear in the Telecommunications Act – are inapplicable. This failure to carry out the necessary legislative amendments is the cause of legal uncertainty among all those involved. I made known my opinion on this matter in my last activity report (see No. 15.1.1 of the 27th Activity Report), and I have informed political decision-makers of the need to take action on several occasions.

The current division of powers between the Federal Network Agency (*Bundesnetzagentur*, BNetzA) and the BfDI is another area where changes are needed. As things currently stand, I have no legislative powers to enforce the data protection provisions of the Telecommunications Act. Instead, I am obliged to forward my complaints to the BNetzA. I believe that this arrangement is incompatible with European primary law, according to which compliance with data protection provisions must be monitored by independent authorities (Article 8(3) of the Charter of Fundamental Rights of the European Union and Article 16(2) sentence 2 of the Treaty on the Functioning of the European Union (TFEU)). The BNetzA, which falls under the jurisdiction of the German Federal Ministry for Economic Affairs and Energy (*Bundesministerium für Wirtschaft und Energie*, BMWi) and is therefore bound by the latter's instructions, does not meet these criteria. This legal position means that the enforcement of data protection law in the areas covered by the Telecommunications Act is, to a large extent, divorced from the activities of the data protection supervisory authorities, e.g. under the aegis of the EDPB.

The urgently required reforms that have been called for on many occasions are still pending.

In a similar vein, I regret to say that no significant progress has been made in terms of reforming the European legal framework for electronic communications. I have already reported in detail on the revision of the ePrivacy Directive, which is to be replaced by an ePrivacy Regulation that is directly applicable in the Member States (see No. 17.2.4.1 of the 26th Activity Report and No. 15.1.2 of the 27th Activity Report). The European Commission adopted a proposal for an ePrivacy Regulation on 10 January 2017, and the draft report

by the committee responsible (the European Parliament's Committee on Civil Liberties, Justice and Home Affairs) was adopted in plenary on 26 October 2017, but the Council of Ministers needs to agree on a general approach before the necessary trilogue negotiations can take place. The dossier has been debated by the Council since mid-January 2017, so far without success.

In my last activity report, I criticised the gradual undermining of the provisions of the ePrivacy Regulation to the detriment of data protection (No. 15.1.2 of the 27th Activity Report), and this continues to be a problematic feature of the current debate. From a data protection perspective, it is advisable to be cautious when granting telecommunications service providers powers to process electronic communications data, and clear and exhaustive rules must be adopted on the purposes of these data processing operations.

Directive (EU) 2018/1972 establishing the European Electronic Communications Code must be transposed into national law by 21 December 2020. In the context of the ECJ judgment of 13 June 19 (C-193/18), this Directive is vitally important for the area of telecommunications. The ECJ found that a web-based e-mail service such as Gmail does not constitute a telecommunications service within the meaning of the Telecommunications Act. At least on a temporary basis, these services are therefore no longer covered by the scope of the Act. The European Electronic Communications Code will clarify the situation in this respect, and introduce the new concept of "interpersonal communications services". I strongly recommend that the legislator should take prompt action to make the necessary amendments.

As part of the debate on the safety of 5G mobile phone networks, a revised list of security requirements pursuant to Section 109 TKG was adopted; the list was drafted by the BNetzA in collaboration with the Federal Office for Information Security (*Bundesamt für die Sicherheit in der Informationstechnik*, BSI) and the BfDI. The goals pursued in this connection included not only safeguarding the confidentiality of telecommunications, but also guaranteeing network availability. For example, the current draft calls for the certification of critical components and the imposition of obligations on the supplier. This is a good idea in principle, but its feasibility remains to be proven. It goes without saying that the certification of high-complexity components that are updated frequently is anything but trivial. The draft also calls for network monitoring, which I regard as

a double-edged sword. On the one hand, monitoring of this kind would require infrastructure that would also make it possible to monitor certain traffic – albeit only for the purpose of detecting faults; on the other hand, the absence of monitoring would leave providers in the dark about attacks within their networks. The legislative requirements of Section 100 (1) and (2) TKG must also be taken into account in this respect. Significant improvements can be reported in other areas, for example the long-overdue requirement for VoIP (Voice over IP) data to be transferred in encrypted form. A comparable requirement for e-mail services is not on the cards, however, since they do not qualify as telecommunications services as the law currently stands.

I recommend that the provisions of the Telecommunications Act and the [German] Telemedia Act (*Telemediengesetz*, TMG) should be brought into line with the GDPR.

5.3 Security legislation

Legislative initiatives in the field of security are particularly likely to be associated with incursions into citizens' rights. Speaking generally, it would be useful to evaluate the powers that have previously been granted to determine whether they are, in fact, still necessary.

This reporting period was similar to previous years in that a significant number of draft bills were tabled that granted the security authorities more extensive powers of intervention, without any parallel evaluation of the powers already held by these authorities.

Particularly in the context of the holistic approach to the extent of surveillance in society developed by the Federal Constitutional Court back in 2010 (*Überwachungsgesamtrechnung*), I take a very critical view of this "drip, drip" accumulation of options for intervention by the security authorities. I am therefore calling on the parties involved in the legislative process to declare a moratorium on security-related legislation.

This would involve carrying out a stock-taking exercise before introducing further powers for the security authorities, in order to determine which of the powers that have already been granted are, in fact, still required. Based on my experiences from

previous fact-finding and control visits, I am inclined to believe that a fair number of the options currently available for the processing of personal data by the security authorities could be removed without any major detriment to the work of these authorities (see No. 6.7.1). An evaluation process of this kind, carried out separately from any assessment under data protection law, would also increase the public's confidence that the legislative provisions allowing incursions into fundamental rights will, in fact, be designed – to the best of the legislator's ability – as broadly as necessary and as restrictively as possible.

[I recommend declaring a moratorium on security-related legislation and launching an evaluation of the powers of intervention granted to the security authorities in order to identify any implementation deficits.](#)

5.3.1 Customs Investigation Service Act

I reported in detail on the amendments to the [German] Customs Investigation Service Act (*Zollfahndungsdienstgesetz, ZFdG*) in my 27th Activity Report (No. 9.1.4), as well as the concerns regarding data protection law that I had raised during the consultation process. The Act that has since been adopted by the German Bundestag is intended to transpose the provisions of the Data Protection Law Enforcement Directive and the landmark ruling by the Federal Constitutional Court on the Federal Criminal Police Office Act.

The Act provides for new powers of intervention for the customs investigation authorities, particularly in the field of safety, and therefore reflects the current political ethos of granting ever-broader powers to the security authorities. The customs investigation service was previously able to deploy undercover investigators only for law enforcement purposes; in future, this will also be possible for safety purposes.

At the same time, the customs investigation service will be granted the power to identify and locate mobile phone cards and telecommunications terminal equipment for safety purposes, for example using IMSI catchers or WLAN catchers. A special legal basis has also been created for source telecommunications surveillance, which will make it possible in future for the Customs Criminological Office (*Zollkriminalamt, ZKA*) to record

communications before they are encrypted or after they have been decrypted.

The new Customs Investigation Service Act requires me to carry out extensive new mandatory controls at least every two years, not only in respect of particularly intrusive domestic investigative measures, but also in respect of data transfers and, more generally speaking, access to personal data within the customs investigation information system. Controls play a key compensatory function in the case of interventions that take place without the knowledge of the individual in question. The BfDI will need to expend a large amount of staffing resources on these new tasks, and the legislator has granted my request for a staffing increase in the federal budget for 2020.

5.3.2 Code of Criminal Procedure

Over the past decade or so, the Federal Government has presented draft bills relating to the [German] Code of Criminal Procedure (*Strafprozeßordnung, StPO*) at regular and repeated intervals, and these bills invariably give rise to issues pertaining to data protection law. One could reasonably query whether the Federal Government is basing these draft bills on an overarching plan of any kind, since it is not uncommon for provisions to be amended that have only recently been revised.

I would like to cite the draft “Act on the modernisation of criminal proceedings” as an example, which sounds like a major step forward, but is in fact merely a compilation of individual amendments that are intended to accelerate the criminal prosecution process but that in reality – among other things – water down data protection rules. In particular, I object to the legislator's proposals to expand the scope of DNA analysis, on the basis of which the investigative authorities would be permitted to analyse DNA samples for the additional purpose of drawing conclusions about an individual's eye, hair and skin colour and biological age, marking the first time that analysis of the coding region of DNA has been permitted. Evaluation of the coding region represents an intrusion into the core area of personality rights, however. Since this is protected by the guarantee of human dignity and is therefore inviolable, the Federal Constitutional Court has previously permitted access only to the non-coding region. What is more, it is far from certain that these new DNA analysis options will, in fact, help investigators to solve crimes, and their value as investigative tools should not be overestimated. As the technology

currently stands, DNA analysis can never be used to identify an individual with 100% accuracy on the basis of the characteristics referred to in the draft bill. It can be used only to estimate probabilities, and these probabilities are by no means as high as one might believe after reading the draft bill. For example, it is generally agreed that predictions relating to mixtures of colours (e.g. mid-brown hair, slightly darker skin, green eyes) are a lot less reliable and are unlikely to deliver the promised benefits during the investigative process. Instead, they carry the risk of encouraging premature decisions to proceed down what might be an incorrect investigative pathway. It is impossible to predict the impacts of analysing the coding region, and granting access to it may well be akin to opening a Pandora's box. It is to be feared that allowing access to this region now will encourage people to assume that, in future, as the science improves, access might also be granted to other information such as hereditary diseases, character attributes or (alleged) genetic predispositions to criminal behaviour.

5.3.3 The dark web

The Federal Council has tabled a draft bill on the prosecution of criminal offences taking place on the dark web; it would appear that the bill has been well received by legal and political circles, but it has not yet been adopted. However, its vague formulations mean that its scope covers lawful behaviour as well as illegal marketplaces.

Anonymisation and encryption are key building blocks in privacy-friendly technical design. For that reason alone, definitions of criminal offences that are worded too broadly must be rejected, since they would otherwise run counter to the principles of data protection.

The websites described by the draft bill as punishable under criminal law do not need to be operated for the purpose of "committing" criminal offences, but merely for the purpose of "promoting or facilitating the commission of criminal offences". It is sufficient for a provider simply to create an environment that is conducive to criminal offences of this kind, without needing to operate a website for the specific purpose of committing them. This distinction may mark a decisive turning point, since the relevant provisions could be interpreted broadly to cover all websites that anonymise Internet traffic or allow password-protected or encrypted exchanges of data (e.g. social networks). After all, it is impossible to rule out the possibility that these websites might be used for criminal activities.

Only criminal actions should be sanctioned under criminal law, and the legislator must therefore provide a precise description of the behaviour that forms the subject of a specific criminal provision. In my opinion, the proposed legislation does not do this satisfactorily. Although the explanatory memorandum for the draft bill states that this approach was chosen with a view to solving evidentiary problems, it is debatable whether this was a good idea. In addition to these vague and broadly worded descriptions of offences, it will also be admissible to carry out investigations as soon as an initial suspicion exists, meaning that the number of innocent parties who find themselves being investigated will increase.

The very introduction to the draft bill contains a sweeping assumption that the Tor network is equivalent to the dark net. This assumption is incorrect: the Tor software is also used for privacy-friendly browsing on the "normal web", and it is a vital tool for politically persecuted persons, journalists and whistleblowers in many different countries. There are well-founded and legitimate reasons for using the Tor browser for "normal" surfing, since it is virtually the only way to use the Internet without being tracked.

5.4 Census 2021

The [German] Act on the Implementation of the Census in 2021 (*Gesetz zur Durchführung des Zensus im Jahr 2021, ZensG 2021*) entered into force on 3 December 2019. In future, the census will be carried out without public surveys, using only cross-sectoral evaluations of a large number of different registers. The details of this legislation continue to raise problems from the perspective of data protection law.

Since 2011, EU law has made it mandatory to carry out a census every 10 years, and the 2021 census is again designed as a register-assisted population survey. The census results are obtained from information that is already available in registers (e.g. the registration authorities), public surveys (e.g. a building and housing census or sample-based household surveys) and surveys at addresses with special areas (collective living quarters and shared accommodation). The Federal Constitutional Court found that this procedure was constitutional in its ruling on the [German] Act on the register-assisted census in 2011 (*Gesetz über den registergestützten Zensus im Jahre 2011, ZensG 2011*), handed down on 19 September 2018.

Once again – as was the case with the 2011 census –

no convincing evidence has been adduced that might indicate why anonymous surveys cannot, as a general rule, be carried out among residents of collective living quarters. This would safeguard the legitimate interests of data subjects for whom the very fact of residing in such an establishment represents highly sensitive data. Similarly, no evidence has been provided that would justify the requirement – which applies once again – for the collection of data on legal affiliation with a religious community under public law, particularly since this represents a step beyond the EU provisions on the part of the legislator.

The 2021 census differs from previous censuses in that the task of managing the entire data pool has been centralised for the first time within the German Federal Statistical Office (*Statistisches Bundesamt*). Cooperation between the Federal Statistical Office and the statistical offices of the *Länder* on the preparation, execution and evaluation of the census – to say nothing of the provisions of the GDPR – makes it particularly important to regulate clearly and distinctly the differing responsibilities of the statistical offices under data protection law. This is of vital importance, not least in the interest of safeguarding data subjects' rights, but I regret to say that the legislator did not follow my proposal in this matter. In view of this and other considerations, I will closely monitor the further preparations for the census and its execution, with a particular focus on compliance with the legislative provisions concerning the erasure of data that are no longer required.

A further focus of my work will be the move towards a future register-based census carried out entirely without public surveys; the first steps in this direction have already been taken. This development will give rise to new data protection challenges, in particular as regards the need to link up information from existing and newly created registers in different sectors.

5.5 Modernisation of registers within Germany

The modernisation of registers within Germany is one of the most important projects under the Federal Government's digitalisation strategy. One of the central building blocks in this project is the introduction of a unique identifier for every citizen, but identifiers of this kind are associated with significant risks. It will be a huge challenge to devise a solution that complies with data protection principles and is therefore

constitutional.

My last activity report contained a discussion of the modernisation of registers (see No. 9.2.2 of the 27th Activity Report). The National Regulatory Control Council (*Nationaler Normenkontrollrat*, NKR) published an opinion in 2017 investigating the advantages and feasibility of modernisation, and the current coalition agreement put the project back on the agenda. The parties agreed that unique and cross-register identifiers should be introduced with a view to the restructuring and networking of Germany's landscape of registers. The Federal Government believes that personal identifiers are the most obvious solution. Identifiers of this kind are generally designed as numbers or combinations of numbers and letters.

The concept of a personal identifier is not a new one: many countries such as Sweden, Denmark or Estonia already use systems based on unique identifiers. Back in the 1970s, the Federal Government also made plans to introduce a system of this kind, but in a ground-breaking ruling on the census in 1983 (ref. 1 BvR 209/83), the Federal Constitutional Court stated unequivocally that the introduction of a personal identifier carried an incalculable risk that a citizen's entire personality might be recorded and catalogued. The Federal Constitutional Court explicitly referred to identifiers as a negative example.

The very fact of introducing a personal identifier increases the risk that all the data which the State holds about an individual will be brought together in one place, and the incursion into the citizen's right to informational self-determination takes place at the time when the data are supplied. Use of the personal identifier merely exacerbates its severity. Checks must therefore be carried out to determine whether there is any possibility of implementing a system based on unique identifiers in a constitutionally compliant manner.

Although there are many obstacles that must be overcome before this project can be implemented, both politically and from the perspective of data protection law, several levels of government have taken on the challenge. Following a number of different decisions by the Standing Conference of the Interior Ministers of the *Länder* (*Innenministerkonferenz*) and the IT Planning Council (*IT-Planungsrat*) over the period up to mid-2019, the BMI was assigned the task of drafting several bills relating not only to the introduction of a unique identifier, but also to the use of such an identifier for digitalised administrative services. A good example of a use case that is already at the development stage

is the Simplified Services for Parents (*Erleichterte Leistungen für Eltern*, ELFE) project, the aim of which is to ensure that citizens no longer need to supply proof of identity or income on multiple separate occasions. Instead, the correct details matching up to the individual citizen are retrieved from the relevant data registers operated by the administration using a unique identifier.

The BMI asked the data protection supervisory authorities of the Federal Government and the *Länder* for advice at an early stage in connection with the various workshops, working groups and expert groups that were organised. This pleased me greatly, not least in view of the importance of the topic and its complexity from the perspective of data protection law. Regrettably, however, the consensus that emerged early on from these bodies was that the Federal Government's preferred solution would be to use the tax identification number and the associated master data record.

I believe that this is a problematic and concerning approach, one that is equivalent in all respects to the solution that the Federal Constitutional Court singled out for criticism back in 1983. The DSK accordingly published a resolution in September 2019 rejecting a uniform identifier of this kind.

The question therefore remains as to whether any form of personal identifier can be compatible with constitutional law. An affirmative answer to this question could be given only if a system were devised that reduced or prevented the risk of cataloguing while, at the same time, guaranteeing public involvement, providing full transparency about all state-initiated transfers of data and incorporating structural barriers (to cross-sectoral identification and any resulting exchanges of data) that inherently prevented the risk of excessive aggregation. Of course, care would also need to be taken to avoid undermining the original goal of improving digital exchanges of data between the authorities.

One potential solution would be to use sector-specific identifiers or identifiers that have been restricted in some other way, and this is the option that the DSK has endorsed. A sector-specific identifier would have further advantages from the perspective of data protection law. For example, if a unique identifier were to fall into the wrong hands, the miscreants would find it significantly easier to access data from all areas of the data subject's life. A sector-specific identifier would allow them access only to a single area, and the consequences of data loss would at least be mitigated somewhat.

This is not enough on its own, however. A fully transparent system (as called for above) is necessary to redress the power imbalance between the citizen and the State. Data subjects that cannot comprehend the data processing operations taking place in the background would be at a disadvantage compared to state authorities engaging in opaque activities. It would be unclear which data had already been collected by the State, when these data had been accessed and by which authority. This is undoubtedly an accurate reflection of many of the Federal Administration's day-to-day activities, and the point applies just as much today as it did back in 1983 – and so the Federal Constitutional Court's ruling is just as relevant now as it ever was.

It will not be possible to devise a unique identifier that complies with the principles of constitutional law until this power imbalance is overcome, and the data protection supervisory authorities believe that certain measures are particularly important in this respect. Data subjects should be entitled to the highest possible level of transparency about flows of their personal data, since they need this information to exercise their rights effectively. It should also be possible to retrieve the data stored by the authorities easily and in a straightforward manner, and individual data subjects must be involved before the exchange of data commences.

I recommend using several sector-specific identifiers when modernising registers instead of a uniform personal identifier.

5.6 Legislation in the field of healthcare and social welfare

The BMG drafted a particularly large number of bills during the reporting period. Some of the 23 draft bills that were tabled were very extensive and required lengthy consultations.

As a preliminary comment, it should be noted that the BMG – in common with other departments – is paying less and less attention to the provisions of the Joint Rules of Procedure of the Federal Ministries (*Gemeinsame Geschäftsordnung der Bundesministerien*, GGO) regulating cooperation when drafting bills, in particular cooperation with the BfDI. This is particularly unfortunate given the large number of draft bills and the urgency of the issues raised from the perspective of data protection law.

Legislative initiatives of particular note during the reporting period included the [German] Digital Healthcare Act (*Digitale-Versorgung-Gesetz*, DVG), the [German] Implant Register Act

(*Implantateregistergesetz*) and the [German] Measles Protection Act (*Masernschutzgesetz*).

The Digital Healthcare Act: health apps on prescription and amendments to research-related provisions

Media attention focused especially on the provisions of the Digital Healthcare Act amending the rules on the “data transparency register”, which were originally established by the [German] Act on the Modernisation of the Statutory Health Insurance Funds (*Gesetz zur Modernisierung der gesetzlichen Krankenversicherung*, GMG) of 30 November 2003 (Federal Law Gazette I, p. 2190) and revised thoroughly for the first time by the [German] Act on Improvements to Healthcare Structures under the Statutory Health Insurance Funds (*Gesetz zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung*) of 22 December 2011 (Federal Law Gazette I, p. 2983). Following the enactment of the [German] Data Transparency Regulation (*Datentransparenzverordnung*) of 10 September 2012 (Federal Law Gazette I, p. 1895), the relevant database was subsequently established within the DIMDI and named the “Information System for Healthcare Data” (see No. 11.1.3 pp. 141 et seq. of my 24th Activity Report). The Digital Healthcare Act modified the reporting channels and increased the amount of data stored in the database for research purposes. I welcome the fact that data are no longer forwarded with the immutable part of the health insurance fund number, as was originally planned. Instead, the data sets are now assigned a “supplier pseudonym” by the statutory health insurance funds before they are forwarded, and the trust centre then converts it into a final pseudonym with the aim of making it even more difficult to re-identify these sensitive data. Following the adoption of the new regulations, the data will now be forwarded in parallel to both the Federal Insurance Office (*Bundesversicherungsamt* – since 1 January 2020: Federal Office for Social Security (*Bundesamt für soziale Sicherheit*)), for the purpose of the risk adjustment scheme, and the Research Data Centre (*Forschungsdatenzentrum*), ensuring that the data are significantly less out-of-date. The data previously made available to an unchanging group of parties with access permissions were typically four years old. Although the legislative provisions on this topic have not been amended, I assume that the expansion into a Research Data Centre provided for by law means that the BMG will now appoint a separate trust centre. The previous special arrangement, according to which the DIMDI would act as both the trust centre and the data-holding authority, was agreed with the BfDI as an absolute

exception owing to the special circumstances. The Digital Healthcare Act expanded the options for the use of data for research purposes, but additional safeguards under data protection law were provided by means of additional access criteria and an explicit duty to criminalise under Section 307b SGB Volume V, as well as the option of preventing access to data under Section 303e (6) SGB Volume V.

The basis for work during the legislative procedure relating to the Digital Healthcare Act was the previous holding of data by the DIMDI, which in future (as a Research Data Centre) will also supply data for research via PC workplaces for guest researchers. Research data centres of this kind are not unusual in the academic sector and are generally set up in line with data protection requirements. This made it all the more surprising when the BMG decreed by ministerial order – only two weeks after the official adoption of the Digital Healthcare Act, scheduled to come into effect from 2 January 2020 – that the DIMDI should be dissolved and that its tasks (and therefore also the database) should be transferred to the BfArM. The procedural concerns that exist in connection with this course of action are significant; from the perspective of data protection law, it is also particularly problematic that a database containing highly sensitive data should be transferred to the BfArM, which (pursuant to Section 303e (1) (16) SGB Volume V) is itself an authorised user of this database, and which (pursuant to Section 303e (3) SGB Volume V) should receive access to sensitive health data only on the basis of an application – an application which it must now check itself.

I subsequently exercised my supervisory powers by informing the DIMDI and the BfArM that use of the research database is prohibited pursuant to Section 16 (1) BDSG in conjunction with Article 58(2)(d) GDPR unless I have been presented with a data protection impact assessment pursuant to Article 35 GDPR indicating how the rights and freedoms of insured parties will be protected. The BMG responded promptly with a ministerial order suspending the relevant parts of the order to dissolve the DIMDI and prohibiting the supply of data to authorised parties.

I succeeded in making heard my objections to a cross-provider directory of insured parties. It might be convenient for insured users to be directly forwarded or linked to the administrative portal of the competent health or nursing care insurance fund on the basis of such a directory, but an assessment under data protection law reveals that the aggregation of data on this scale runs counter to

the principle of data minimisation within the meaning of Article 5(1)(c) GDPR and the principle of necessity within the meaning of Article 6(1) GDPR.

The Digital Healthcare App stipulates that health apps can now be prescribed by doctors or approved by health insurance funds, meaning that their costs can be reimbursed by the statutory health insurance funds. I regret to say that many of my suggestions for ensuring that this wholly novel arrangement complied with data protection requirements were ignored. I had urged the legislator to ensure that health apps would be made available to users exclusively within the telematics structure and without the involvement of “app stores”, that the manufacturers or other third parties outside the healthcare sector would not receive sensitive health data about app users, and that no tracking would take place. I also suggested that the data protection and data security requirements applicable to digital health apps should be stipulated in detail in the law. I did chalk up at least one success in this respect: during the approval process for an app, checks will be carried out to determine whether it meets data protection requirements and provides state-of-the-art data security. Nevertheless, the procedure for approval by the health insurance funds and the identity of the controller under data protection law within the meaning of the GDPR need to be clarified in the regulation provided for by the Digital Healthcare Act. Identification of the controller under data protection law in the case of digital apps prescribed by doctors or approved by health insurance funds is particularly important, since it serves as a basis for determining the party against which data subjects can exercise their rights under data protection law and which must carry out the data protection impact assessment that may be necessary in individual cases (Article 35 GDPR).

Collection of data about certain implants under the Implant Register Act

The purpose of the [German] Act Establishing an Implant Register (*Implantateregister-Errichtungsgesetz*) is to merge the specialist implant registers previously operated by professional medical associations. It is the first health register to be based on a mandatory and country-wide reporting obligation (see No. 4.2.2).

Measles Protection Act

As a result of the Measles Protection Act (officially titled the “Act to prevent measles and strengthen vaccination prevention (*Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention*)”), persons working in establishments such as

kindergartens or schools (educators, teachers, daycare staff and medical staff [born after 1970]) are obliged, before being hired or starting work, to provide evidence “[...] that they have received a vaccination protecting them against measles” or to present a doctor’s certificate “confirming that they are immune to measles or that a vaccination against measles is contraindicated for medical reasons”. The same applies to children from the age of one when they start school or kindergarten. In this connection, I was able to push through my suggestion that a simple certificate from a doctor confirming immunity against measles would be an acceptable alternative to a vaccination record proving vaccination against measles. There is no good reason why individuals should be obliged to disclose all vaccinations to directors of kindergartens and schools if they are entirely irrelevant for attending or working in the kindergarten or school in question.

Act Reforming the Medical Services of the Health Insurance Funds

The [German] Act for Better and More Independent Checks (Act Reforming the Medical Services of the Health Insurance Funds) (*Gesetz für bessere und unabhängigere Prüfungen (MDK-Reformgesetz)*) reorganised the medical services of the health insurance funds on the basis of a uniform and separate structure. These medical services provide assistance to the statutory health insurance funds if medical matters need to be assessed, for example when deciding whether to grant benefits, and I welcome the fact that they are now more independent. Many of the enquiries I receive relate to the unclear division of tasks between the health insurance funds and the medical services of the health insurance funds, and the resulting inadmissibility of the related data-processing operations. This new structure should create more certainty when individual cases are handled, *inter alia* as regards data protection concerns.

I also welcome the news that I will be involved in the adoption of guidelines by the new Federal Government Medical Service (*Medizinischer Dienst Bund*) when it has been established, in particular since this corresponds to the procedure followed when decisions are adopted by the Federal Joint Committee (*Gemeinsamer Bundesausschuss*).

Cross-reference:

4.2.2 Implant Register

6.Security

6.1 Cross-border access to data by the security authorities

Three procedures allowing direct cross-border access to data by the security authorities are currently in the pipeline: the CLOUD Act, the eEvidence Regulation and the Convention on Cybercrime. This move away from the principle of international mutual legal assistance that previously prevailed is problematic in several respects from the perspective of data protection law.

6.1.1 CLOUD Act

The CLOUD Act grants US law enforcement authorities extensive access to data held by Internet service providers, regardless of where they are stored, which can result in conflicts of law. According to an initial assessment by the EDPB, direct transfers to US law enforcement authorities outside mutual legal assistance channels are incompatible with many GDPR provisions. A solution may be found in the form of new agreements, but the obstacles are significant.

The CLOUD Act, which entered into force in the USA in March 2018, pursues two goals: firstly, it regulates the conclusion of administrative agreements between the USA and other countries or the EU, on the basis of which both sides will, in principle, be granted access to the personal data stored by Internet service providers in the other country. As the US Government sees it, this primarily benefits the other countries, since the pre-eminence of the US Internet industry means that many foreign law enforcement authorities require data stored in the USA for their own investigations. Secondly, and more concerning, the CLOUD Act also stipulates that US law enforcement authorities will be granted extensive access to data held by Internet service providers under US jurisdiction, regardless of where the data are stored.

This second point is particularly controversial, since provisions of this kind could easily give rise to conflicts of law if the required data were also covered by the scope of another legal regime such as

the GDPR. In an initial assessment, the EDPB took the position that transfers of data to the US law enforcement authorities solely on the basis of the CLOUD Act are unlikely in a typical case to be permissible under the GDPR. Unless it is necessary to protect the vital interests of a data subject, the existing mutual legal assistance procedures should be followed to ensure that data required for criminal investigations are transferred in accordance with the law.

At the same time, the EDPB suggests ways in which the relevant requests for information could be handled in future without giving rise to conflicts of law. In particular, it emphasises the need for a new generation of mutual legal assistance treaties aimed at accelerating the handling of requests and providing a higher level of data protection. Alternatively, the EU and the USA could conclude an agreement regulating these matters; an agreement of this kind is indeed being negotiated at present, but it must incorporate adequate procedural safeguards and a high level of data protection in order firstly to create the necessary legal certainty and secondly to ensure that all parties involved benefit more from the new agreement than from a continuation of the status quo.

6.1.2 The eEvidence Regulation

The term “eEvidence” refers to a proposal for a regulation by the European Commission that would allow European law enforcement authorities to access subscriber data, traffic information and content data directly from telecommunications and Internet service providers in other EU Member States. The orders would also be binding on third-country providers that offer their services in the EU.

The main criticism I voiced in my last activity report related to the lack of involvement of the judicial authorities, at least in the country in which the requested provider is based (see No. 11.1.4 of the 27th Activity Report). Internet service providers should not be solely responsible for determining whether orders are legitimate, since the interests

motivating ISPs and judicial authorities are fundamentally different, as are the obligations imposed upon them. To put it another way, the responsibility for carrying out legislative checks and protecting data subjects should not be transferred (entirely) from the State to private actors. I therefore welcome the proposal by the European Parliament's rapporteur to introduce a procedure for mandatory parallel notification of the judicial authorities in the Member States involved.

A further aim of the eEvidence Regulation is to ensure compliance with third-country regulations that protect fundamental rights in the relevant country and that might stand in the way of the provider's disclosing the requested data. The European data protection authorities have called for the same to apply in respect of third-party legislation governing access to data that falls within the scope of the GDPR. I therefore see it as regrettable that the Member States came down in favour of deleting a much-needed provision regarding the mandatory consultation of a competent body in the relevant third country.

A further problem relates to the authentication of the requesting authority and individuals, since it is difficult to imagine how this would be possible. A provider might be contacted by a great many authorities in other Member States on the grounds that the national law of the respective Member State permits them to do so as an investigative authority in criminal proceedings.

The eEvidence Regulation had not yet reached the stage of trilogue negotiations between the European Parliament, the European Commission and the Council by the editorial deadline for this document. The questions raised should, however, be settled over the next few months during the discussions that will be carried out in this connection.

6.1.3 Convention on Cybercrime

The issues raised by the eEvidence Regulation under data protection law (see No. 6.1.2 above) are also the focus of the negotiations currently under way on a Second Additional Protocol to the Convention on Cybercrime.

The Convention on Cybercrime is a treaty on crimes committed via the Internet and other computer networks; it was negotiated under the aegis of the Council of Europe, but is open to countries that are not Council members. So far, a total of 64 countries have signed the Convention, including Australia, Canada, Israel, Japan, Senegal, Tonga, Turkey and

the USA.

The two provisions that are most important from the perspective of data protection law, and that are being debated at present in connection with the Additional Protocol which is currently being negotiated, relate to cross-border access by security authorities to both user and traffic data. The first provision regulates the requirements for direct cross-border access by law enforcement authorities in one signatory state to data held by providers in another signatory state. This is problematic from the perspective of data protection law since a variety of differing (and, in some cases, greatly differing) legal systems and data protection standards apply in the 64 signatory countries.

The second provision in the Additional Protocol is intended to speed up the traditional mutual legal assistance procedure between the law enforcement authorities. This might lead to solutions that deliver accelerated mutual legal assistance as well as an improved level of data protection. In my opinion, some of the factors that should be taken into account in this respect include the need to place narrow restrictions on the categories of data that can be accessed, and to ensure that requests are submitted or approved by independent authorities. The involvement of the judicial authorities in the countries where the providers receiving data requests are based is another important factor.

At the same time, however, it will be possible to carry out a final assessment of the Additional Protocol only once the data protection provisions negotiated in connection with the Convention on Cybercrime are published. Approval of the draft Additional Protocol is currently scheduled for the end of 2020.

Cross-reference:

6.1.2 The eEvidence Regulation

6.2 “Smart” video surveillance pilot project at Berlin-Südkreuz railway station

The first subproject, which involved testing the facial recognition software, has been completed; the second subproject is now at the evaluation phase. The creation of a legal basis for biometric facial recognition in the police sector would not only lead to far-reaching incursions into fundamental rights, but would also mark a socio-political watershed.

In No. 9.3.3 of my 27th Activity Report, I reported on the pilot project launched by Deutsche Bahn AG, the BMI and the Federal Police (*Bundespolizei*), which was the first of two subprojects. The Federal Police tested biometric facial recognition software from several companies, and then published a final report. In my legal opinion, the outcome is extremely concerning for several different reasons. I have fundamental reservations about the design of the test methodology, which means that the results are of limited value. As I see it, the percentage of individuals that are misidentified is much too high for across-the-board use in a live environment (see https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile).

Analysing a data subject's biometric data and then carrying out searches to determine whether these data appear in various databases represents a significant incursion into that individual's fundamental rights. As yet, no legal basis has been created for the use of biometric video analysis, and the requirements under constitutional law that would apply to any legal basis of this kind are very high – for good reason.

The introduction of biometric facial recognition as a surveillance technology deployed in day-to-day policing should certainly be regarded critically from the perspective of data protection law and social policy. Digital surveillance cameras are already an omnipresent feature of our landscapes, and the necessary data are therefore already available. What is more, experience has shown that the legal restrictions on access to data that are initially imposed are gradually scrapped over time. If the legislator allows the police to use biometric facial recognition, there is a very real risk that the opportunities for surveilling the public using biometric characteristics will be expanded step by step – a development that cuts to the very core of our coexistence within society. A broad social debate must be held on the wisdom of creating such an opportunity. Biometric video analysis is not simply one more tool in the police's arsenal.

After the first subproject on facial recognition was completed in 2018, the second part of the test – which has since also been completed – commenced on 18 June 2019, again involving the use of software for “smart” video analysis. Situations such as people prone on the ground, abandoned pieces of luggage, gatherings of people or people entering restricted areas were simulated – in some cases using actors – to determine whether the software would detect these individual hazards and notify them to the control centres operated by Deutsche Bahn AG and

the Federal Police. According to the manufacturer, biometric features of the software such as facial recognition were disabled during these tests. The Federal Police and Deutsche Bahn AG are currently evaluating the data that were generated and findings that were made. I will carry out my own in-depth assessment of the test outcomes once they have been forwarded to me.

I was able to provide advice in the run-up to this part of the testing process, and was able to express my concerns about the design of the test and the information provided to the general public. For example, the original idea of using the entire concourse of the railway station to carry out the test on the relevant days was abandoned at my suggestion, and it was carried out only in certain demarcated areas. I was also able to ensure that more signs were displayed telling the public what was happening, and that these signs were positioned in more visible locations.

[I recommend that video surveillance with biometric facial recognition should not be used in public spaces.](#)

Cross-references:

No. 9.3.3 of the 27th Activity Report

6.3 Police 2020

Following the legislator's announcement of a new Federal Criminal Police Office Act, the Federal Government announced a major IT project entitled “Police 2020” in 2018. The BMI presented the project roadmap to me and promised that I would be involved in the discussions on the individual planning stages.

I reported on the “Police 2020” programme in my last activity report (see No. 9.3.4 of the 27th Activity Report). The aim of this project is to bring about far-reaching changes in the IT landscape of the German police, with the goal of creating a joint “data house” between the police forces of the Federal Government and of the *Länder*. A centralised storage system is intended to avoid data being stored in multiple different systems by different police forces.

The BMI and the Federal Criminal Police Office (*Bundeskriminalamt*, BKA) hope that implementation of this programme will result in higher-quality data, improved access to the data that are required by the police and the bundling of resources within the BKA as the central service provider. Finally, the planned data house would provide uniform logging and analysis options.

As I see it, however, the end result of all this might be broader and more disseminated availability of data within the police information network – which might be problematic if data have been stored about an individual who has done nothing to warrant said storage, for example, such as victims, witnesses or persons who initially came under suspicion but were exonerated in the further course of proceedings because the suspicions could not be substantiated or confirmed.

At the start of the year, I was invited to a BKA event which involved carrying out tests on the data house (referred to as a data consolidation proof of concept – PoC). The details of these tests revealed data processing operations that did not meet the criteria for relevance to the information network set by the Federal Criminal Police Office Act. I very much welcome this initiative by the BKA at an early stage of the procedure, but I regret to report that – after expressing major concerns about the system that was being tested – I was not invited to visit the BMI on any further occasions.

Nevertheless, at the end of the year, the BMI provided me with a progress update for the “Police 2020” project. One of the points that emerged in this connection was that the ambitious name – “Police 2020” – refers to the start of the changes to the IT landscape rather than a fully implemented project. The BMI and BKA are still at the early stages of this journey, and are currently working on a “development plan” for the new IT architecture. The first phase of this plan will culminate in an interim solution, based on centralising the case handling systems of the police forces of the *Länder* (as well as the case handling system eFBS and the exhibit system AMS) to the greatest extent possible. The INPOL-Z database and the Police Information and Analysis Network (*Polizeiliche Informations- und Analyseverbund*, PIAV) are to be merged into a single network.

As was previously the case within the police’s IT landscape, each participating body will be responsible for its own data (“principle of ownership”). With a view to ensuring compliance with the provisions of police law and data protection law, the BMI is developing an attribute-specific and dynamic access and role permissions concept that drills down not only to each data set, but to each individual piece of data. In the long term (a time frame of 10 years or more, according to the BMI), a second phase will result in the merging of all of these systems into a single overall system to be used regardless of the field of activity, albeit with a customised interface. All case-specific and *Land-*

specific data would then be available solely via the joint data house.

The BMI and BKA face major challenges in connection with this project, both in technical terms and from the perspective of data protection law. I have not yet been supplied with a detailed written concept for an assessment under data protection law, but the BMI – following a constructive exchange of views – has agreed to involve me on a regular basis in future.

6.4 Storage of PNR data

Since 29 August 2018, the Passenger Information Unit (PIU) set up by the BKA has stored the passenger name records forwarded by airlines. Data of this kind may potentially be collected for passengers travelling on all flights arriving in or leaving Germany across Schengen borders or intra-EU borders. Since this date, hundreds of thousands of passenger name records have been accumulated. The legal basis for the collection and evaluation of these data is the Passenger Data Act, which transposes the EU Passenger Name Record Directive into German law.

I have already expressed criticism of the processing of PNR data in my previous activity reports (see No. 13.5.4 of the 22nd Activity Report, No. 2.3.2 of the 26th Activity Report and No. 1.3 of the 27th Activity Report). At the very latest since the ECJ published its Opinion on the agreement envisaged between Canada and the European Union on the transfer of Passenger Name Record data on 26 July 2017, there has been much debate over whether Directive (EU) 2016/681 of the European Parliament and the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive) is compatible with the Charter of Fundamental Rights of the European Union. The same applies to Germany’s Passenger Data Act.

In its Opinion, the ECJ clearly rejected the concept of retaining PNR data for all air passengers over long periods of time without specific grounds for doing so. As regards the transfer of PNR data to Canada, the ECJ stated that the date of departure should be used as a basis for determining the permissible retention period. As regards air passengers in respect of whom no risk has been identified as regards international terrorism or serious transnational crime on their arrival in Canada and up to their departure from that country, the ECJ believes that the original objective pursued by the

transfer of data has been fulfilled, and further retention of the data would be inadmissible. The ECJ believes that further retention would be admissible only if there were objective evidence in specific individual cases from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada.

In my legal opinion, the ECJ's deliberations on the inadmissibility of the long-term retention of PNR data for all air passengers without valid grounds are just as applicable to the Passenger Name Record Directive and the Passenger Data Act. I have therefore called on the Federal Government and, together with other European data protection supervisory authorities, on the European Commission to make amendments to these pieces of legislation, but little evidence of willingness to do so has been discernible to date.

Actions relating to the retention of PNR data are pending before courts in Germany as well as in other EU Member States, and the Belgian Constitutional Court has referred several queries regarding the compatibility of PNR rules with the Charter of Fundamental Rights of the European Union to the ECJ for a preliminary ruling. I welcome these efforts to shed some light on the situation. In particular, the ECJ must make a landmark ruling on whether and for how long PNR data can lawfully be retained without valid grounds for the purpose of preventing and prosecuting terrorist offences and other serious crimes.

6.5 Queries submitted to the BfV before awards of public funding

Before public funding is awarded to private entities, the federal ministries submit queries to the BfV with a view to ensuring that the relevant funding is not misused by anti-constitutional organisations. There is no adequate legal basis for the involvement of the BfV and the associated processing of personal data.

As part of its integrated approach to the fight against extremist and terrorist organisations, the BMI – in its Haber-Diwell Decree of 2017 – stipulated that public funding was also relevant in terms of internal security. The types of funding in question include programmes targeted at young people, education, development, the environment or integration policy. To ensure that this funding is not misused by anti-constitutional organisations, the federal ministries are asked to submit queries to the BfV to check

whether the latter holds any information about the organisation in question that might be relevant in terms of constitutional protection. After carrying out the necessary checks, the BfV informs the federal ministries whether it holds any information on the organisations, persons or events referred to in the application that might be relevant in terms of constitutional protection. The BfV's response plays a vital role in determining whether public funding is granted to an applicant.

Given the far-reaching impacts this may have on the parties affected by a query and the resulting relevance in terms of fundamental rights, special provision under law should be made for these problematic data processing operations involving the BfV.

There are currently no provisions with the force of law that explicitly allow the involvement of the BfV for the purpose of checking whether any information is held about specific individuals that might be relevant in terms of constitutional protection, with a view to preventing the misuse of public funding. Provisions that merely take the form of a decree do not form a sufficient basis for such involvement.

Broadly speaking, other relevant general provisions of law or blanket clauses that might apply to the BfV, such as Section 8 (1) sentence 1 or Section 10 (1) of the [German] Federal Constitutional Protection Act (*Bundesverfassungsschutzgesetz*, BVerfSchG), cannot be used as a legal basis since there must be actual indications that the BfV is affected in the performance of its statutory tasks. At the time when a federal ministry submits a query to the BfV with a request for the latter to carry out checks, however, there is no indication that the free democratic basic order or the existence and security of the State will be jeopardised by the granting of public funding. As the procedure currently stands, actual indications of this kind emerge, if at all, only as an end result, and only in relation to the individual parties being checked.

If the legislator believes that it is necessary to use information supplied by the BfV as a basis for taking decisions on the granting of public funding, it must create a corresponding legal basis.

The BMI disagrees with me on this point, and believes that there is no need for further legislation on this matter. It regards Section 3 BDSG in conjunction with Sections 8 (1), 17 (1) and 19 (1) sentence 2 BVerfSchG as an adequate legal basis.

I recommend that an explicit and comprehensive legal basis should be created for the “Haber procedure”.

6.6 Advisory and fact-finding visits to the Federal Intelligence Service

Under the Strategic Initiative Technology (*Strategische Initiative Technik*, SIT), the Federal Intelligence Service (*Bundesnachrichtendienst*, BND) is upgrading its technological skills and capacities to bring them into line with changing circumstances. This was the finding that emerged from my various advisory and fact-finding visits to the intelligence services that took place during the reporting period. The stringent requirements of the Classified Information Order (*Verschlusssachenanweisung*, VSA) mean that I can report on these matters only to a very limited extent, however.

Joint examinations of the purpose and functioning of new IT systems within the BND had already been carried out in previous years, and continued during the reporting period with two additional advisory and fact-finding visits. These visits concentrated on selected systems forming part of the technical redesign of signals intelligence, and I was able to gain far-reaching insights into the collection and further processing of personal data by the BND. These will serve as a basis for the preparation and streamlining of later data protection controls. Further exchanges of information are also planned for the year ahead with a view to expanding this overview of the BND's IT landscape.

6.7 Controls involving the security authorities

6.7.1 Mandatory controls

Regular controls of specific files or investigative measures are mandated by an increasing number of legislative acts at both national and EU level.

I reported on my initial experiences of the various mandatory controls in my last activity report (see No. 14.3.9 of the 27th Activity Report). Once again, I carried out several mandatory controls during the current reporting period; this involved the anti-terror file and the right-wing extremism file, the use of the second-generation Schengen Information System (SIS II) and the admissibility of data retrievals from the European Visa Information

System (VIS) and the European Asylum Dactyloscopy Database (Eurodac).

Anti-terror file and right-wing extremism file controls

In 2019, these files were checked by almost all the security authorities that fall under my jurisdiction, including the BKA, the Federal Police, the Customs Criminal Office (*Zollkriminalamt*, ZKA), the BND and the BfV.

As well as the control relating to the anti-terror file, I also carried out another scheduled control within the BKA, namely that relating to the mandatory control of the right-wing extremism file. No criticisms emerged from either of these controls. What did emerge, however – especially in relation to the anti-terror file – was that the authorities involved are accustomed to exchanging the key information via channels other than the anti-terror file. In particular, the BKA carries out its own investigations to follow up on the information about cases it receives from other authorities via these separate channels. Against this backdrop, I do not believe that these shared files ultimately allow the BKA to perform its tasks more effectively.

I also carried out controls of the anti-terror file and the right-wing extremism file within the Federal Police. As was the case back in 2017, these controls confirmed that both files were designed as tools for initiating communication; despite this, however, information about suspicious activities is exchanged via other channels of communication. In situations involving an immediate risk, the authorities involved find it too cumbersome and ineffective to use the anti-terror file or the right-wing extremism file. Nevertheless, the information is still entered into the files – at great expense in terms of time and human resources – to ensure that it is accessible to other authorities via this route as well.

Similar findings – that other channels of communication and forms of communication are more significant than the anti-terror file in practice – emerged from a further mandatory control of the anti-terror file within the ZKA. A further problem that arose in this connection was that the ZKA on the one hand acts as a controller by storing data in the anti-terror file and independently specifying the requirements for said storage, but on the other hand – since it is not responsible for leading the fight against terror – generally receives only “actual indications” within the meaning of Section 2 of the [German] Anti-Terror File Act (*ATD-Gesetz*) in connection with findings reported by other authorities. The mere fact that data concerning an

individual have already been stored in the anti-terror file is not sufficient. Instead, individual pieces of valid information must be collected from other authorities or otherwise available for the purpose of performing its own tasks, in order to avoid the risk of snowballing data volumes. The ZKA must therefore review all entries in the anti-terror file again and delete entries that have been made solely because another body has stored data about the relevant individual.

The controls of the anti-terror file within the BND that started in 2018 could not be completed in 2019. The data sets that were examined during the controls were found to contain many references to foreign intelligence services. Activities in this sector are subject to the “third-party rule”, which means that the foreign intelligence services involved must be consulted. The foreign partner services have been asked whether it would be possible to notify the BfDI of these data sets as well, but no response has been received to date. An assessment under data protection law of this form of data storage is therefore a long-winded and complex affair, involving a great deal of effort on my part.

Further controls of the anti-terror file and the right-wing extremism file were carried out within the BfV on the basis of my long-standing and successful working relationship with the G10 Commission. Unfortunately, the Federal Government – as was the case during a similar control within the BND in 2018 – prevents the G10 Commission from accessing data in the absence of clear indications that these data relate to G10 activities (see No. 6.7.5). This places obstacles in the way of full and uninterrupted supervision of the BfV. In addition, and as I already mentioned in my last activity report (see No. 9.3.11 of the 27th Activity Report), it continues to be difficult to use the log data for both files for data protection control purposes.

Since there are no signs of readiness to embark on the radical redesign of these files that is long overdue, I still believe that the anti-terror file and the right-wing extremism file – which are also unpopular among the security authorities – should be abolished. Alternatively, the BMI (which is responsible for technical supervision not only of the BKA, but also of the BfV and the Federal Police) should, at long last, reform both files so that they are easier to use for all authorities involved. As things currently stand, both controls and technical and subject-specific updates require a disproportionate amount of effort compared to the functional benefits derived. A reform of this kind would also allow the bodies performing controls to carry out their tasks

more efficiently.

Second-generation Schengen Information System (SIS II)

In 2019, I carried out a control within the Federal Police that followed on from a control I had performed in 2018 regarding preventive alerts on persons issued by the police for the purpose of refusing entry and stay, during which I had identified shortcomings as regards the criteria for data storage that had been documented, especially in connection with the necessary predictive decisions. The control I carried out this year revealed that the Federal Police are actively working on a uniform administrative approach in this area. Parts of the documentation still fall short of being self-explanatory, and so I recommended improvements again in this respect. Another criticism I raised this year related to log data, since the retention periods did not comply with EU requirements in all respects, and the data were not available at short notice for the purpose of the data protection control. The Federal Police promised to make improvements in this connection.

I carried out random checks of alerts on persons posted by the BKA to determine whether they complied with the applicable legislative provisions, and identified no problems in this respect. The procedural rules on the submission of alerts for arrest and the handling of “hits” were also observed. Future controls will again focus in closer detail on the content and scope of hits. As was the case with the controls carried out within the Federal Police, the main points of criticism raised during these controls related to log data: the log data stored in connection with the history of alerts are retained for too short a period. The BKA has promised to make the changes that are urgently required to bring this period into line with EU requirements.

One of the controls I carried out within the BND during the reporting period related to SIS II. The German intelligence services are permitted to use SIS II only for “covert alerts” pursuant to Article 36(3) of the SIS II Decision in conjunction with Section 17 (3) BVerfSchG in order to track movements, but not, for example, to arrest persons upon entry into the country. The information obtained must be necessary to avert a significant risk posed by the individual in question or other significant risks to the security of the State. I am still in the process of evaluating the sample that was checked, but I can already confirm that the procedural documentation lacks clarity in certain respects.

Retrieval of data from the VIS and Eurodac databases

Over the course of 2019, I carried out controls to determine whether the BKA's retrieval of data from the VIS and Eurodac databases could be considered lawful. Searches of this kind can be carried out under certain conditions for the sole purpose of preventing, detecting or investigating terrorist or other serious crimes. I checked samples from both systems; the legitimacy of the data retrievals was readily apparent in all instances. The documentation concerning data retrievals from the VIS database could be clearer, however, and I issued a recommendation in this respect.

My controls concerning the legitimacy of Eurodac searches within the Federal Police commenced in 2018, and documentary shortcomings were detected at an early stage of the process. After evaluating additional documents and log data, it was found that the documentation did not always clearly show whether the requirements for admissibility of the retrieval had been met. I voiced criticism of this failure in 2019, since it violates the rule-of-law obligation to maintain proper files based on Article 20 (3) GG. The Federal Police have since responded to this criticism by taking steps to overcome the documentary shortcoming I highlighted, and these appear appropriate as things currently stand. I will review during future controls whether they have delivered the required outcome.

Conclusion

Regular mandatory controls play a vital role in enforcing compliance with the relevant provisions of data protection law, but they also take up a lot of man-hours. In the medium and long term, it is important to avoid adverse impacts on areas that are not explicitly regulated but that have proven to be problematic – and perhaps even more so – under data protection law than the areas in which mandatory controls are prescribed. The supervision of activities by the security authorities is a vitally important area of action, but the criteria for balanced control measures must always be met; the additional staffing resources approved by the Bundestag for the BfDI will make a significant contribution in this respect.

Cross-references:

6.7.5 Fragmentation of the supervisory landscape for the intelligence services

6.7.2 Source telecommunications surveillance within the BKA

The BKA has brought its activities more into line with the requirements under data protection law regarding the transparency of its telecommunication surveillance measures. During a data protection control, I was also able to inspect sections of the source code.

I have previously spoken critically about source telecommunications surveillance measures, *inter alia* in connection with the technical features and risks of the software products used. The outcome of the discussions held between the data protection authorities and the security authorities was a more stringent list of requirements. Even at that stage, I insisted on full transparency regarding compliance with these requirements, which are based on the powers granted by law, and range right through to disclosure of the software product's source code. Situations of this kind often present certain difficulties: it is difficult to identify and control the precise method of functioning on the one hand and the side effects on the other hand. With this in mind, I criticised the absence of documentation for the surveillance software used at the time, and the virtual impossibility of inspecting the source code in order to check whether the legal requirements had been met.

The BKA has since expended a significant amount of effort on pressing ahead with a proprietary version of the source telecommunications surveillance software, with the aim of remedying the lack of transparency regarding the source code's compliance status I had previously criticised. During a control performed in 2019, I therefore examined the software development process to determine whether it was designed in such a way as to allow the requirements and legal standards to be referred to and checked at each stage of development. I was provided with a special version of the software for the purpose of this examination which could be used on a monitored device, and which offered a sample range of features from abstract requirements management through to details of the source code.

As a result of this examination, I was able to gain assurance that the BKA can clearly demonstrate compliance with the requirements at each individual stage of the process, and that it can, in principle, design the special software components of the surveillance system in a compliant manner. I had previously carried out a use test which revealed that the software was restricted to the surveillance of ongoing telecommunications.

6.7.3 The BKA's handling system

During one of my controls, I raised concerns about the BKA's case handling and file management systems. The case handling system does not distinguish adequately between the different purposes for which the police authority processes personal data, which means that the scope of access rights and search options is defined too broadly. In addition, no provision has been made for the tagging of data from domestic investigation measures.

According to the opening order (*Errichtungsanordnung*) that has applied to date, the purpose of the case handling system is to create and handle documents for individual cases, as well as to document incoming and outgoing messages, documents and cases and manage existing ones. Finally, it can also be used to search for individual documents and cases.

Yet the system I was shown not only offers features that go well beyond those described above, but also fails to comply with certain basic requirements. In total, I raised six complaints as a result, which are set out below.

The case handling system per se

The case handling system does not distinguish adequately between the different purposes for which the Federal Criminal Police Office process personal data, even though purpose limitation is a key basic principle of data protection. The starting point for related deliberations should be the reason why an individual's data might have been stored in police files, and these reasons can be many and various. Data may be stored when someone is convicted as an offender, but they may also be stored when someone is a victim or witness of a crime. It follows that different benchmarks must apply under data protection law, and all of the Police Acts (*Polizeigesetze*) adopted by the Federal Government and the *Länder* therefore distinguish between three basic purposes for which the police authorities process data:

1. **For the performance of tasks:** Police authorities are permitted to store data for the purpose of performing a task. The scope of the data they may collect in order to do so, for example from witnesses or victims, is extensive. Access to these data must be restricted, however, and only those working on the case may be allowed to view them. Generally speaking, access should therefore be restricted to the competent organisational unit. Once a case has been closed, there are, in principle, two different reasons for continued storage of the data.

2. **As a precaution ("police memory"):** The police can continue to store personal data if they have adequate cause to do so. For example, the Federal Criminal Police Office Act states that data concerning suspects or individuals who have been charged may be stored for precautionary purposes if a documented negative finding indicates that they are likely to commit further criminal offences. Save a few exceptions, the BKA may not store data belonging to witnesses and victims for this purpose.
3. **As documentation:** Data are stored for documentation-related purposes as a basis for later checks to determine whether the police authority has acted legitimately. For example, such checks may be carried out if victims complain that the police intervened too late or if a suspect believes that their communications have been intercepted for no good cause. **Case handling** is a similar and related purpose, aimed at ensuring that cases and documents can be retrieved again.

It follows that the case handling system does not adequately differentiate between these three fundamental purposes. In particular, the data processed for case administration and documentation purposes are not strictly separated from the data processed for the purpose of performing tasks or handling cases. During the control, I was not able to ascertain from the individual data sets whether the BKA had stored them to perform a specific task or to document police activities. I also criticised a related shortcoming, namely that access rights had not been appropriately assigned according to the purpose of processing. As a basic principle, data stored for the purpose of performing tasks should be accessible only to the employees responsible for the relevant tasks, and special justification must be provided for any exceptions, since there would otherwise be a risk of undermining the principle of purpose limitation. For example, if all the data stored for documentation purposes were available during searches, the hits returned might include individuals whose data should not be stored for the purpose of preventing risks, including individuals for whom no negative finding has been made.

The case handling system should not therefore be used as a comprehensive search system, but it contains a feature labelled "File circulation" (*Dateienrundlauf*), which allows users to search through all of the data contained in this system. Only a small number of data types – those labelled as

“restricted search only” – are excluded. In principle, users within the BKA who are familiar with criminal investigations could search through all of the data held by the police, including data whose processing lies outside their jurisdiction. At the same time, they can also search through other police data assets and additional registers, such as the INPOL police information system and the Federal Central Register (*Bundeszentralregister*, BZR). Frequent use is made of this feature, and in my opinion one of its impacts is that people are sometimes stored in the case handling system merely in order to be able to carry out a “File circulation” search. Storing data about individuals for the sole purpose of carrying out a search in a database is a flagrant violation of data protection principles, and so I voiced my criticism of this feature.

It is also important to clarify which data need to be stored in the first place for documentation purposes. For example, the BKA receives a large number of criminal tactical queries (*kriminaltaktische Anfragen*, KTA) from the *Länder*. In many cases, no further measures are taken on the basis of these queries; they are merely stored in the case handling system. The exact purpose of these documentation efforts is questionable, and it ultimately means that the rules on precautionary storage are circumvented. These queries should be properly stored in a file held by a central department, since they are held on a precautionary and searchable basis. In order to do so, the statutory requirements must be met in each individual case.

There was a great deal of variability in terms of time limits within which data must be reviewed for relevance and erasure. The BKA has not put in place uniform criteria as guidance for determining these time limits in respect of the case handling system. The law, however, states explicitly that documentation is permitted only on a “time-limited” basis. This should be clarified in greater detail, because otherwise BKA employees will continue to lack a benchmark for their decisions. I also issued a criticism regarding this matter.

A further criticism I issued related to the fact that I was unable to identify an option for labelling data that had been collected using particularly intrusive measures, even though labels of this kind should have been in place for some time pursuant to the provisions of the Code of Criminal Procedure. Despite my criticisms, there are a lot of good things to say about the technological solutions deployed in this system, which was designed as a proprietary product by the BKA. This approach allowed the BKA to present me with information on assigned access rights and comprehensive overviews of data

distribution at short notice for the purpose of the data protection control, for example. I believe that the shortcomings I have identified relate more to internal organisational rules than to the system’s technical design.

File management

The legitimacy of police activities must be comprehensively documented, but the case handling system contains only extracts of cases. Most correspondence and annotations are stored solely as files on shared drives, which does not provide an adequate safeguard that the files are stored in full and protected against manipulation. It also does not meet the requirement of proper documentation (*Aktenmäßigkeit*), since in order to do so it is essential for the documents to be stored in the correct sequence and for it to be possible at all times to identify the individual decision-making channels and the relevant authors within the authorities; otherwise, the contextual links will be broken. Proper documentation also requires systematic logging of individual documents, including the assignment of reference numbers, even if every last file is stored on a departmental drive. I criticised this as an infringement of the principles of proper file management.

As a result, I recommend that the features of the electronic file management system should be redesigned from the bottom up. In particular, the juxtaposition between file management and the documentation of police activities should be restricted to the absolute minimum necessary. End-to-end documentation of the legitimacy of police activities must be consistently safeguarded.

6.7.4 Data protection and security clearances

The provisions of data protection law must also be taken into consideration in the context of the law on security clearances.

During the reporting period, I carried out controls within three companies responsible for security vetting on behalf of the BMWi. These companies carry out security clearances for the purpose of preventive individual security vetting. During previous controls, I had highlighted infringements relating to the maintenance of security files (No. 9.3.14 of the 27th Activity Report), and these were present again during my controls this year. Examples include patchy file-keeping, the inclusion of documents in files that should not have been there and failure to comply with the statutory deadlines for destruction and erasure. In most cases,

these infringements could be attributed to a lack of awareness on the part of the security officers responsible. As a result of my efforts, most of the infringements relating to file management were remedied either during my control visit or in the immediate aftermath. I did not therefore issue any criticisms.

I would especially like to emphasise the fact that I was able to establish constructive working relations with all of the companies within which I carried out controls. The security officers were amenable to the suggestions I made during my visits, and agreed to implement them or to remedy the shortcomings I had highlighted.

During the reporting period, I also carried out controls in respect of the BfV's management of security and security clearance files for job applicants. Once again, I identified various infringements of data protection law relating to individual aspects of the security clearance procedure, the management of security files and compliance with the deadlines for destruction and erasure. As a result of my comments during the controls, however, the BfV removed all of the documents from the files that should not have been there and carried out checks to ensure compliance with the deadlines for destruction and erasure. This meant that most of the infringements relating to file management could be remedied either during the controls or in their immediate aftermath.

I find it regrettable that the BfV makes use of the opportunity to inspect data subjects' personnel files, and I am still in discussion with the BfV on this topic.

6.7.5 Fragmentation of the supervisory landscape for the intelligence services

The supervisory landscape for the intelligence services in Germany is fragmented. I have made repeated calls to the legislator asking for the number of controls carried out in this area to be stepped up, and I am also trying to avoid gaps in supervisory practice by means of discussions and contacts with other supervisory bodies.

As I noted on repeated occasions in my past activity reports, the fragmentation of the supervisory landscape for the intelligence services results in gaps in supervisory practice that need to be remedied both through legislative measures and through measures on the ground (see No. 9.1.5 of the 27th Activity Report). I take my obligation to cooperate with other supervisory bodies very seriously, and will continue to carry out joint

controls of the anti-terror file and the right-wing extremism file with the G10 Commission, in line with consistent past decisions by the constitutional courts.

Following amendments to the explanatory memorandum for Section 26a BVerfSchG, the Federal Government has finally granted me access to G10 data; at the same time, however, the G10 Commission was prevented from inspecting data originating from G10 measures during a control carried out within the BND in 2018 in relation to the anti-terror file. The Federal Government upheld this stance in 2019, and once again prevented the G10 Commission from inspecting data during a joint control in relation to the right-wing extremism file within the BfV (see No. 6.7.1), on the grounds that Section 15(6) sentence 5 of the [German] Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, G10-Gesetz) – unlike Section 26a BVerfSchG – had not been amended. The Federal Government does not appear to believe that there is any reason to make amendments of this kind. A constitutional complaint is pending before the Federal Constitutional Court, and I hope that, in its ruling, the latter will make unambiguous statements about cooperation between the BfV and G10 Commission, with a view to increasing the level of legal certainty and clarity for all parties concerned.

The G10 Commission is not the only supervisory authority with oversight over the intelligence services; others include the Independent Committee (*Unabhängiges Gremium*), which exercises oversight over the BND in the field of foreign-foreign signals intelligence. I believe that there is scope for cooperation in this respect too with a view to avoiding gaps in supervisory practice.

With that in mind, I met with the Independent Committee for an initial exchange of ideas, during which I set out my views on the matter. The Independent Committee places a great deal of emphasis on strictly upholding its duty of confidentiality. In my opinion, it is not only a good idea but – in the light of consistent past decisions by the constitutional courts – absolutely necessary to amend the law to allow active exchanges of information so that seamless supervision can be exercised over the BND in the field of signals intelligence and any subsequent processing of personal data.

As a result of the fact that it exercises oversight over the intelligence services, security authorities, public bodies and private companies, the BfDI is currently

a repository of wide-ranging specialist and methodological expertise in the area of data protection controls. The budget legislator has recognised the need for strong data protection supervision in the area of the security authorities (police and intelligence services), and backed this up with a generous amount of funding earmarked for staffing increases. Cooperation between the BfDI as a centre of expertise and the other supervisory

bodies with their powers and capabilities is likely to serve as a sound foundation for carrying out appropriate controls.

Cross-reference:

6.7.1 Mandatory control

7. Bundestag

7.1 The Bundestag's internal pass and access system

In 2018, the Council of Elders (*Ältestenrat*) of the German Bundestag decided that an electronic internal pass system should be introduced for individuals visiting or working within the Bundestag. An internal pass of this kind authorises the individuals to enter the Bundestag properties and contains an RFID chip for contactless reading at their entrance gates.

The internal pass system has been in operation since early 2019, and is based on an implementing concept that incorporates my recommendations. In March 2019, I carried out a fact-finding and control visit in relation to this system.

Only one card number (AccessID) is stored on the internal pass. Contactless reading of this number takes place at the entrance gates of the Bundestag properties so that the associated data set (which is stored in a centralised file) can be accessed. The security personnel are then given access to the individual's details and photograph for the purpose of comparing them against the text and images printed on the pass, solely as a means of confirming the individual's identity. A separate cryptographic module is used for the RFID chip to prevent unauthorised access to the internal pass.

Based on the documents that were shown to me, the discussions I held and my in-person visit, I believe that the internal pass and access system design complies with the state of the art as regards the protection of personal data. The organisational rules on data subjects' rights are adequate, and the necessary amount of information is provided to data subjects. In keeping with the principle of data minimisation, the data that have been collected are required for the purpose of granting access to the Bundestag properties, and the planned deadlines for erasure are appropriate. A point of particular note is that access is not logged, meaning that movement tracking is not possible.

7.2 Controls in relation to the Bundestag police

In No. 21.1 of my 25th Activity Report, I called for the adoption of a formalised legal basis for the activities of the Bundestag police. Although this police force carries out its work appropriately, I voiced criticisms about its processing of police data, because there continues to be no legal basis for these data processing operations.

I carried out an advisory and control visit to the Bundestag police back in January 2019, which focused primarily on the use of personal data to confirm the identity of individuals entering the Bundestag properties and buildings and the issuing of internal passes. The Bundestag police uses the Federal Central Register and the INPOL police information system managed by the BKA in both instances. As a basic principle, the procedure followed by the Bundestag police when carrying out these checks is appropriate, and I issued no criticisms in this respect. The checks are carried out for the purpose of safeguarding proper parliamentary operations – as a protected asset – and the constitutional bodies involved in these operations.

At the same time, however, there is still no formal basis for the exercising of these police powers. In my opinion, the proprietary powers of the Bundestag President regulated in Article 40 (2) GG are not an adequate legal basis for exercising police powers that infringe upon the fundamental right to informational self-determination. I therefore believe that a need exists for a constitutionally compliant legal basis that is set out in adequate detail and also implements the Law Enforcement Directive. I therefore voiced formal criticisms of the processing of data by the police to the Bundestag President. I am happy to report that the President has, in the meantime, notified me that he has asked the Bundestag Administration to draft a bill clarifying the legal basis for the work carried out by the Bundestag police, inter alia in the area of data protection.

8. Other individual topics

8.1 Third-country transfers

One of the side effects of globalisation is an increase in cross-border data processing and transfers of personal data to third countries across borders. Over the past year, the debate on the impacts of Brexit on data transfers between the EU Member States and the United Kingdom has been a particular focus of attention. In addition, transfers of personal data from the EU to the USA have remained on the agenda.

8.1.1 Consequences of Brexit for data transfers

The United Kingdom's decision to leave the EU also has implications in terms of the transfer of data between the EU Member States and the United Kingdom, which will become a third country under data protection law after its departure.

I made it known early on that controllers and contract processors should make provisions for Brexit, *inter alia* in the field of data protection. Although it has since become clear that the United Kingdom will leave the EU on the basis of a withdrawal agreement, controllers and contract processors should continue to monitor developments.

In terms of data protection law, the United Kingdom will become a third country when it leaves the EU on 31 January 2020. Nevertheless, the GDPR will remain in effect in the United Kingdom until 31 December 2020. It follows that there is no need for special safeguards when transferring data to the United Kingdom during this transitional period. UK-based companies will also continue to benefit from the one-stop-shop principle until that date.

The Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom states that the European Commission will endeavour to adopt the necessary adequacy decisions by the end of 2020, with a view to facilitating the continued free flow of data. If this were to prove impossible and the planned transitional period were not extended, the

United Kingdom would immediately become a third country, and the GDPR would no longer apply there. From this point onwards, controllers and contract processors wishing to transfer personal data to partners in the United Kingdom would need to take the appropriate safeguards pursuant to Chapter V GDPR in connection with these data transfers.

I will continue to provide updates on the latest developments concerning Brexit at www.bfdi.bund.de/brexit.

8.1.2 Proceedings in the Schrems II case

Standard contractual clauses serve as a basis for data transfers to the USA. The ECJ is expected to hand down a ruling on these clauses during the first half of 2020 in the "Schrems II" case.

The ECJ ruling that was handed down in October 2015 and that declared the Safe Harbor arrangement to be invalid – the "Schrems decision" (case C-362/14) – caused a sensation. It made it necessary to negotiate a new agreement with the USA, and the outcome of these negotiations was the Privacy Shield. The ECJ has now been tasked with adjudicating on data transfers within the Facebook Group. These proceedings are referred to as "Schrems II", and their outcome could have much further-reaching consequences. This time, the issue at stake is whether the applicable standard contractual clauses serve as a sufficient basis for transfers of personal data to the USA. In practice, these standard contractual clauses are the most popular way of supplying evidence that transfers of data to third countries are protected by the necessary appropriate safeguards. The significance of the case can be deduced from the fact that the oral hearing before the ECJ's Grand Chamber lasted eight hours. The EDPB – represented by its Chair and a BfDI employee – was also invited to this hearing for the first time.

If the ECJ were to find that the extensive powers granted to the US intelligence services or the unsatisfactory means of legal redress available to EU citizens prevented use of the currently applicable standard contractual clauses, it would no longer be

possible to cite them as appropriate safeguards. This would have an enormous impact not only on transfers of data to the USA, but in all probability also on transfers to other third countries. The outcome of the oral hearing in the Schrems II case suggested that there was also a possibility that the ECJ would rule on the validity of the Privacy Shield at the same time, since the European Commission's findings on US law in connection with the Privacy Shield may be binding on the data protection authorities in the event of a decision on the legitimacy of data transfers based on standard contractual clauses. As intimated by the ECJ during the oral hearing, these authorities should not take any measures that contradict the Commission's findings.

The ECJ has announced that its decision will be handed down in the first six months of 2020, and the opinion delivered by the Advocate General on 19 December 2019 might be an indication of the general thrust of the Court's ruling. In this opinion, the Advocate General recommends that the standard contractual clauses should remain valid. He stated that, when used as a facilitating tool for transfers, they offered sufficient safeguards for personal data. Nevertheless, companies should suspend transfers of data to third countries if the legislative provisions that apply in the third country make it impossible to comply with contractual obligations. The data protection authorities would then also be obliged to prohibit transfers of this kind.

According to the Advocate General, there was no need to rule on the validity of the "Privacy Shield" decision. In the event that the ECJ chose not to follow his recommendation and to issue such a ruling, he set out, in an abundance of caution, the reasons that had led him to question the validity of the "Privacy Shield" decision.

8.1.3 Developments relating to the EU-US Privacy Shield

Implementation of the "Privacy Shield" EU-US data protection agreement by the US Administration has improved, but there are still some major problems.

Additional joint checks of the EU-US Privacy Shield were carried out during the reporting period, and BfDI employees participated in these checks as part of the EDPB delegation. Positive developments on the US side were identified during these checks. For example, the Privacy and Civil Liberties Oversight Board, which plays a vital supervisory role, once again has a full roster of members. The Board

advises the President and the executive branch on the protection of citizens' rights in the fight against terror, and has far-reaching rights of inspection for the purpose of performing its tasks. In addition, a new Privacy Shield Ombudsperson has been appointed, whose task will be to field complaints from European citizens relating to instances in which US security authorities have accessed their personal data.

Nevertheless, the EDPB believes that these first tentative steps towards improved oversight over the US security authorities must be followed up with more decisive action. For example, the EDPB asked the Privacy and Civil Liberties Oversight Board to make available additional reports on access by the US security authorities to European citizens' personal data. Another problem that has not yet been resolved is that the US authorities are still not carrying out checks to determine whether the Privacy Shield-certified US companies are, in fact, complying with the relevant rules.

It also still remains to be seen whether the Ombudsperson can actually guarantee effective legal protection within the meaning of Article 47 of the Charter of Fundamental Rights of the European Union; this matter has been referred to the European Court of Justice for clarification within the framework of the Schrems II case (see No. 8.1.2).

These and other proceedings pending before the ECJ in connection with the Privacy Shield will clarify in more detail which framework conditions are imposed by the Charter of Fundamental Rights of the European Union on transatlantic data flows.

Cross-reference:

8.1.2 Schrems II

8.2 The Online Access Act

The Federal Government is hard at work on measures to implement the Online Access Act. This list of measures to be implemented under this Act currently includes 575 administrative services offered by the Federal Government, the *Länder* and the municipalities that must be fully digital by the end of 2022.

As I explained in No. 9.2.2 of my 27th Activity Report, citizens and companies should have access to all administrative services offered online at an administrative portal of their choice without having to identify themselves more than once ("once-only principle"). The method by which users log into their accounts is of crucial importance as far as use

is concerned, and depends on the level of protection required for the relevant administrative service. The EU's eIDAS Regulation distinguishes between three assurance levels: "low", "substantial" and "high". Administrative services with a "low" assurance level (registration with user name and password) and a "high" assurance level (registration using the online identification function of the personal ID card and the electronic residence permit) have been offered digitally to date. The identification data may be stored permanently in the user account only with the user's consent.

For the purpose of implementing the "once-only principle", the Online Access Act specifies the data necessary to identify a natural or legal person, i.e. the core set of data required. This set of data serves as a connecting link for cross-authority administrative procedures. The data stored by the various authorities can be joined up on the basis of this identity management system.

A cross-departmental identification platform must be designed to comply with data protection principles, which gives rise to brand new challenges. Certain quarters have called for a unique personal identifier to be introduced – or the tax identification number repurposed – and used across the board, in the interests of implementing the once-only principle. Yet this would make it possible to track data subjects across all areas of public life, and to carry out comprehensive and detailed profiling of them. The Federal Constitutional Court believes that such comprehensive profiling is anti-constitutional. In the event of data leaks and cyber attacks, a unique personal identifier also increases the risk that unauthorised persons could re-identify citizens from these data.

It is important to ensure that citizens using services under the Online Access Act have and retain control over their data in full and at all times. For example, it might be possible in future for citizens to submit a one-off application for a social security benefit with a single click of the mouse, instead of submitting multiple applications or requesting information from several different bodies as they have previously been required to do. The necessary processes would automatically be triggered following single-time authentication of the applicant. A topical example is the Simplified Services for Parents project, the aim of which is to allow parents to submit a single application for both child benefit (*Kindergeld*) and parental allowance (*Elterngeld*).

From the perspective of data protection law, however, this user-friendly system must not mean

that the individual data processing operations are "black boxed" as far as the applicant is concerned. There are two different approaches to increasing transparency in this respect, as described below.

The first alternative is to continue walking the applicant through each step of the application via an app or a web browser. The forms would be displayed one after another, but would no longer need to be filled out individually, since the system would populate them using data from the relevant sources. The processes taking place in the background could be explained at the same time as the forms were populated. This would provide citizens with the opportunity to carry out checks before they click to confirm and submit the forms (a step for which they hold final responsibility).

Alternatively, consideration could be given to the option of a "data protection cockpit", or a specially designed website – similar to the privacy pages of social networks – that would increase transparency for citizens while still making it possible to trigger all the processes involved in an application with a single click. Key considerations in this respect include the need to gain the user's consent to the exchange of data (in compliance with data protection requirements), and the need to provide applicants with detailed information about exchanges of data belonging to them. In a data protection cockpit model, this would be possible only by retrospectively displaying and explaining the individual processes that took place in the background.

Both of these alternatives guarantee an adequate level of transparency in terms of access to information on the way in which the authorities use data and exchange personal data between themselves, but they differ as regards the level of control exercised by applicants. The data cockpit alternative would make applications quicker and simpler, but the step-by-step alternative gives citizens greater control.

Regardless of which option is ultimately deemed to guarantee the necessary level of transparency, I will ensure that the new legal basis required, while reducing red tape for citizens and companies thanks to a streamlined and more user-friendly design, does not lead to a worsening of personal data protection.

The Federal Government, under the leadership of the BMI, is planning to launch a "Federal Portal" (*Bundesportal*) for the purpose of implementing the Online Access Act. A pilot version of this portal went online during the reporting period, under enormous time constraints. Some of the deadlines set for

checking the documents forwarded to me were extremely short, and I have not yet been able to complete these checks. I would ask to be involved in future work as early as possible so that I can perform my tasks with the diligence required.

[In connection with services under the Online Access Act, I recommend that citizens should be provided with a user-friendly opportunity to learn about and monitor the data processing operations that are taking place.](#)

8.3 Unencrypted e-mails

The secure processing of personal data is a fundamental requirement. Even if data subjects consent to unencrypted e-mail traffic, this does not release controllers from the obligation to take appropriate technical and organisational

measures to protect personal data against unauthorised disclosure.

Both analogue and digital data handling systems must be designed to be secure. Based on the checks I have carried out and the complaints I have received from citizens, however, the fact that different standards apply in this respect is detrimental to data protection. For example, a wide range of different public bodies and companies send unencrypted e-mails containing sensitive data belonging to citizens, and this practice is especially problematic when it involves health data that merit particular protection pursuant to Article 9 GDPR. The confidentiality issues associated with unencrypted e-mail communications are not a secret. In terms of protecting confidentiality, unencrypted e-mails are the digital equivalent to the analogue practice of sending someone a

Encryption as an “appropriate technical measure”

Pursuant to Article 5(1)(f) GDPR, personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (“integrity and confidentiality”). The specific technical and organisational measures that need to be taken depend on the level of risk to the rights and freedoms of the data subjects affected by the data processing operations. The more sensitive the data (whereby the categories of personal data referred to in Article 9 GDPR, such as health data, are regarded as particularly sensitive), the higher the requirements that apply in terms of the protective measures to be taken.

End-to-end e-mail encryption does not necessarily need to be used for each electronic transfer of personal data – it is merely one possible way of ensuring appropriate security, albeit a significant one for data transfers. Other possibilities include the option of e-mailing documents as password-protected archives, for example. At the same time, however, care must be taken to ensure that the encryption technique used is adequately secure, and that secure passwords are also used. The password required for decryption must also be transferred securely, which typically requires a separate channel of communications. A failure to encrypt the e-mail – and in particular the actual text of the e-mail to which the archived file is attached – means that an appropriate level of security cannot be achieved. Under certain circumstances, however, seamless encryption of the entire transfer path can deliver an appropriately secure solution. Online retrieval of protected data via an encrypted connection is a well-established and doable approach for senders and recipients alike. As noted above, the necessary access variables (login, password) must be forwarded using a different secure channel of communications. In many cases, e-mails are particularly insecure because even transmission encryption is lacking when they are sent through the Internet. In technical terms such encryption would be possible, but several providers have failed to take this step in recent years, and improvements in this respect are therefore necessary within Germany’s network landscape.

Since the required level of protection must also be determined on the basis of the gravity of the risk to data subjects’ rights and freedoms, exceptional cases are conceivable in which unencrypted e-mail communications might be permissible. For example, this would apply to unencrypted e-mail notifications concerning the uploading of sensitive data to a protected environment (an existing account accessed with a login and password, for example).

postcard. If you would choose a sealed envelope rather than a postcard to send the information in the analogue world, you should therefore also choose an encryption method when sending an e-mail.

In recognition of the risks posed to the confidentiality of communications in this area, many parties are attempting to legitimise data transfers of this kind in practice by asking data subjects to agree or consent to “open” communications of this kind.

The GDPR states that consent is a potential legal basis for the processing of data in conformity with data protection principles. Pursuant to Article 6(1) GDPR, however, this relates to the lawfulness of the personal data processing operation, and not to the statutory obligation incumbent upon controllers to comply with the necessary technical and organisational measures. If public bodies were allowed to renounce their legislative obligations on the basis of a “voluntary” decision by a data subject, this would represent an infringement of their duty to uphold the rule of law pursuant to Article 20 (3) GG.

It is also debatable whether consent can even be deemed to have been granted voluntarily if an authority requires consent from a citizen for a particular method of data processing.

In my opinion, consent of this kind is neither voluntary nor compliant with data protection requirements, and it can, under no circumstances, be used to legitimise the sending of personal data in unencrypted e-mails.

A legislator-endorsed reduction in the level of data protection?

In spite of the concerns I expressed during the legislative process, the Fiscal Code was amended with effect from 18 December 2019 to allow tax authorities to send unencrypted e-mails to citizens containing data covered by tax secrecy requirements, provided that consent has been obtained from all the parties involved.

In the opinions I provided to the Federal Government and the Finance Committee (*Finanzausschuss*), I pointed out that this arrangement infringed the provisions of EU law, since the GDPR does not allow national exemptions in respect of the security of processing.

I recommend that the public bodies of the Federal Government should ensure that e-mails containing personal data are always encrypted.

8.4 Misuse of data by the Federal Employment Agency’s Job Board

Private employment agencies are also permitted to post vacancies on the Job Board (*Jobbörse*) operated by the Federal Employment Agency, provided that there is a real vacancy to be filled. They are not permitted to post a general advertisement for the purpose of collecting job hunters’ data and building up a pool of applicants. During the reporting period, however, this was exactly what happened as a result of misuse of the Job Board.

A report published by the public service broadcaster Südwestrundfunk (SWR) on 2 May 2019 alerted me to the fact that the Job Board is being misused by several “private employment agencies” to collect applicant data from Job Board users. In order to do so, these agencies post large numbers of vacancies that do not correspond to real jobs. When data subjects applied for these jobs by submitting documents, they were contacted by the “private employment agencies” and asked for consent to forward their data to other potential employers. If they consented, their data were sold to third parties.

After becoming aware of the accusations and after carrying out its own investigations into the matter, the Federal Employment Agency deactivated 46 suspicious “employer accounts”. In addition, criminal charges were brought by both the Federal Employment Agency and the BfDI against one of the “private employment agencies” responsible for perpetrating this misuse.

The Federal Employment Agency – after consulting me – also took steps to enhance the level of user data protection. Since mid-August 2019, the Job Board has been configured in such a way that vacancies posted by private employment agencies are shown only to users who have deliberately activated this option. Following a recent change, users can also see whether a specific vacancy has been posted with the support of the Federal Employment Agency.

All of the vacancies uploaded to the Job Board are reviewed automatically. The algorithm used for this purpose has already been adjusted to check for the fraudulent patterns of behaviour, and is constantly being developed further. In addition, 10% of vacancies that are posted are checked manually. It has now become more difficult for employers/job advertisers to access the Job Board; as well as requiring a company number, the Federal Employment Agency may demand additional documents from companies wishing to use the Job Board.

The Federal Employment Agency's Job Board is intended to make it as easy as possible for job seekers to look for vacancies and for employers to look for applicants. It would be to the detriment of users if companies chose not to post vacancies on the Job Board because of excessive red tape and time-consuming authentication procedures, with the end result that fewer jobs were offered. It goes without saying that the Federal Employment Agency must use all the means at its disposal to protect the personal data of Job Board users, and I will continue to support it in this respect. At the same time, however, all data subjects should be vigilant about the processing of their data. If further consent is requested or a notification is received that data are to be transferred to third parties for no apparent reason, the data subjects in question should contact the Federal Employment Agency immediately. The latter investigates suspicious cases and deletes employer accounts if they violate the Job Board's terms and conditions of use.

8.5 Legislation on aliens and asylum

As in previous years, there were many changes in this area of law during the reporting period. I made my opinion heard during the departmental discussions and in the course of a hearing before the Committee on Internal Affairs and Community (*Bundestagsausschuss für Inneres und Heimat*).

One of the most significant of these many legislative procedures relates to the [German] Second Data Exchange Improvement Act (*Zweites Datenaustauschverbesserungsgesetz*), and I expressed criticisms of this Act during a public hearing before the Committee on Internal Affairs and Community. The DSK also submitted a written opinion to the Committee.

This Act expands yet further the options for retrieving data from the Central Aliens Register (*Ausländerzentralregister*, AZR). Problematic aspects that I have identified in this connection include the broader provision for data retrievals by the ZKA. I cannot see any good reason why these data should need to be accessed in connection with customs investigations. In addition, a further authority – the Bundestag police – has now also been authorised to retrieve data from the Central Aliens Register, even though the reason for these data retrievals continues to elude me. Once again, my criticisms focused on the continuing trend to use the Central Aliens Register number for the unique assignment of data

sets, which I believe may result in a risk of unlawful creation of a single personal identifier.

During the parliamentary process, an obligation for the bodies retrieving data to create an authorisation concept was incorporated into the [German] Central Aliens Register Act (*Ausländerzentralregister*, AZR-Gesetz) to compensate for the streamlining of options for accessing the Central Aliens Register. I will ensure that this obligation has been met during future controls of the bodies entitled to retrieve data.

The number of complaints I receive in the field of alien and asylum legislation continues to be relatively low. Generally speaking, the citizens who contact me require my assistance in connection with access to data held in the Central Aliens Register (in some cases because of a refusal to allow access to these data). The relatively low number of complaints in this area may well be attributable to a lack of familiarity with the channels for lodging complaints, and in particular to a widespread reluctance to embark on this course of action. Certain shortcomings can, however, be identified – and subsequently remedied – only if complaints are submitted. My co-workers drew attention to this fact at an event organised by refugee associations, and called for the data protection supervisory authorities to be consulted more frequently in the event of problems.

8.6 Facebook fanpages

Several court rulings make it clear that the operation of Facebook fanpages in compliance with data protection requirements is not currently possible.

Facebook fanpages continue to be very popular among companies and federal authorities, even though it is almost universally known that Facebook harvests significant amounts of personal data via these pages – and that no one knows exactly which data are collected and what happens to them.

In April 2019, the DSK adopted a “Position on responsibility and accountability for Facebook fanpages and the jurisdiction of the supervisory authorities”. In this document, the DSK explains once again that the information made available to date by Facebook is not adequate. From the perspective of data protection law, fanpage operators act as joint controllers alongside Facebook, and are therefore also accountable to their users under the GDPR, but they cannot fulfil this obligation in the absence of more detailed information from Facebook, and they cannot

therefore operate the fanpage in compliance with data protection requirements. I alerted the companies and federal authorities under my jurisdiction to this point of law in several circulars, and encouraged them to request the necessary information from Facebook.

In late October 2019, Facebook finally published new details of its Internet-based data processing operations, and these details are currently being evaluated by the DSK committees.

I believe that the federal authorities should play an exemplary role in terms of compliance with data protection requirements. The Federal Press Office has assumed responsibility for communicating with Facebook on behalf of the Federal Government, and has informed me that several discussions have taken place with Facebook. The outcomes are sobering, however: even the Federal Press Office, acting as the Federal Government's representative, was sent only information that was already available on the Internet – and not until early November. This attitude on Facebook's part means that the issue will remain on my agenda.

The DSK will discuss a possible course of action to be followed by all the supervisory authorities in future. At any event, the supervisory authorities believe that their position is supported by the Federal Administrative Court's judgment of 11 September 2019 (ref. 6 C 15.18), in which it confirmed that the German supervisory authorities can act directly against fanpage operators, thereby prohibiting the operation of a fanpage. A point that is particularly noteworthy is that the authorities do not need to wait for a decision by the Irish data protection authority, which has jurisdiction over Facebook.

I also stepped up the exchange of information with other European supervisory authorities on the topic with a view to ensuring that supervisory practice within the EU is as uniform as possible.

8.7 Data protection in motor vehicles

Digitalisation-related developments ranging right through to automated and autonomous driving pose challenges under data protection law as well as technical challenges.

The companies involved in developing these automated and connected cars promise that they will make the roads safer and make driving a more pleasurable experience. Yet they must not be

allowed to place inadmissible restrictions on the personal rights and freedoms of vehicle owners, drivers and passengers in terms of the personal data collected while delivering on these promises.

The DSK's position

The DSK believes that particular attention should be paid to the following points during the technical development of new vehicles.

- Any data collected during vehicle operation are influenced by the specific use of the vehicle and are therefore personal. This means that there are no data that are 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.
- Wherever possible, personal data must be processed in the vehicle itself. In the case of connected vehicles, data subjects must have complete control over access to vehicle data and data generated in the vehicle.

Dialogue with the German Association of the Automotive Industry

The dialogue between the DSK and the German Association of the Automotive Industry (*Verband der Automobilindustrie*, DVA), which began in December 2014, led to a first result on 26 January 2016 with a joint declaration on aspects of data protection law in conjunction with the use of motor vehicles (available at www.bfdi.bund.de/entschliessungen). The manufacturers and suppliers represented by the German Association of the Automotive Industry 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 constitute 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. I will also pay close attention to the question of whether vehicle data are, in fact, collected and processed only with the consent of the owner and, where appropriate, the driver and co-driver. Data of this kind can provide far-reaching insights into the driving behaviour of vehicle users, for example. Sovereignty over vehicle data must, therefore, remain entirely in the hands of vehicle users.

Questions I raised with the VDA during the reporting period related, in particular, to the processing of video and audio signals in the vehicle environment that is necessary for the development of automated and autonomous driving. Self-learning systems that need to be trained with huge volumes of real-life video and audio data so that they can guarantee an appropriate level of safety in all traffic situations play an important role in this respect. It follows that, in order to avoid endangering human life or health during the development of autonomous and highly automated driving using self-learning systems, it may be necessary to process large volumes of video and audio data for technical reasons. As part of the dialogue with the VDA, and together with my counterparts from the *Länder*, I emphasised the importance of complying with the provisions of data protection law during the development of highly automated and autonomous driving. Previous conversations with the manufacturers on this topic have been constructive. We are currently working on a joint declaration enshrining the requirements and guidelines of data protection law.

Automated and connected driving

Increasing digitalisation in the automobile and the transport sector makes cybersecurity and data protection increasingly important issues in this area. For example, I advise the “Round Table for Automated and Connected Driving” set up by the German Federal Ministry of Transport and Digital Infrastructure (*Bundesministerium für Verkehr und digitale Infrastruktur*, BMVI), which brings together representatives from industry, academia, insurance organisations and consumer protection groups. This round table provides answers to issues that arise from technical developments in order to make automated and connected 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 [German] Act on the Digitalisation of the Energy Transition (*Gesetz zur Digitalisierung der Energiewende*), which should also apply 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 connected vehicles should be able to communicate with other vehicles, the backend systems of manufacturers or third parties only 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. In this connection, I expressly support the European Commission’s efforts to establish a standard based on non-discriminatory access to vehicle data and data generated in the vehicle via a secure vehicle-based telematics platform, perhaps following the model of smart meter gateways.

Car-to-car communication

Car-to-car communication will play a huge role in the future of private transport. 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 principles of data minimisation and data avoidance are 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 counterparts, I therefore appealed to the European Commission to adequately consider the requirements of the GDPR when developing rules and regulations for smart transport systems.

Outlook

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. Both goals can be achieved at the same time. What is important is transparency, data minimisation and maintaining maximum data sovereignty for data subjects.

I am therefore pleased that my 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.

[I recommend non-discriminatory access to vehicle data and data generated in the vehicle via a secure vehicle-based telematics platform, perhaps following the model of smart meter gateways.](#)

8.8 Data protection and postal services

The digital transformation of postal services can succeed only if the provisions of data protection law are observed. The national legislator has taken steps to increase legal certainty in an evolving postal market by amending the statutory provisions.

The national legislator brought data protection in the field of postal services into line with the provisions of the GDPR by means of the Second Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, which was promulgated in late November 2019. I was able to make suggestions as part of the legislative process. Any sector-specific data protection provisions that had existed up until that point within the [German] Postal Services Data Protection Regulation (*Postdienste-Datenschutzverordnung*) and that were still required alongside the GDPR were transferred to the [German] Postal Act (*Postgesetz*, PostG). This did not affect the principle of postal secrecy under Section 39 PostG, which is protected by constitutional law.

An examination of the postal market makes it clear that the digitalisation of processes is a fast-moving trend. Examples include “Digital Copy” (*Digitale Kopie*) – a product offered by Deutsche Post AG (see No. 8.8.1) – and carrier sequence sorting for increased delivery efficiency (see No. 8.8.2).

8.8.1 Digital Copy

Deutsche Post AG can now also deliver letters digitally. As a basic principle, hybrid mail systems are already possible today, but must be designed to comply with data protection law.

Deutsche Post AG offers a service in this area known as Digital Copy, which allows bulk mailers like banks, insurance companies or even authorities to forward electronic copies of letters that they are sending out in parallel to the hard copies. Deutsche Post AG then checks whether the electronic copies can be sent digitally to the recipient via E-POST digital. If the recipient is a registered E-POST user, the letter is mailed electronically at the same time. I have been campaigning for over 18 months for this procedure to take place within a framework that is admissible under data protection law, with a particular focus on technical and organisational measures. These latter must ensure that digital copies of letters containing potentially sensitive data concerning individuals are used exclusively for the purposes of electronic delivery.

As is the case for the E-POST service, Digital Copy is, first and foremost, a telecommunications service. The provisions of the GDPR, the Postal Act and the Telecommunications Act must therefore be observed when carrying out an assessment under data protection law.

The conclusions I reached on the basis of my discussions with Deutsche Post AG were positive overall, but certain changes still need to be made to bring the service into line with data protection law. These include reducing the length of time for which “digital copies” under Deutsche Post AG’s jurisdiction are retained to the period actually required to provide the service.

Further improvements are also required in respect of technical and organisational measures. For example, the “digital copies” should be accessible only in a very small number of pre-defined cases. End-to-end encryption should also be established as a standard with a view to guaranteeing the confidentiality of communications and the secrecy of telecommunications protected by constitutional law. Encrypted communications are offered only as

an additional option at present.

Evaluation of mail flows

In connection with its Digital Copy service, Deutsche Post AG plans to evaluate flows of mail that could be sent via E-POST in order to identify (and ultimately advertise to) potential new E-POST customers. In order to do so, it has assigned all households to microcells, with each of these microcells containing 6.6 households on average. Letters (or rather mail flows) that could be sent via E-POST will then be counted at the level of these microcells, and the households in the microcell will receive a promotional mailing when a certain threshold is reached. It is highly debatable whether processing data in this way on the basis of a legitimate interest on the part of Deutsche Post AG is lawful. Deutsche Post AG has heeded my concerns in this connection, and has not yet carried out any evaluation of mail flows.

8.8.2 Carrier sequence sorting for increased delivery efficiency

The vast majority of letters have been machine-sorted for many years. A recent innovation in this area is that this sorting process can now also incorporate the position of an individual letterbox within a bank of letterboxes.

Large banks of letterboxes containing many individual letterboxes present significant practical challenges for postmen and postwomen.

Letterboxes follow different (and sometimes confusing) layouts, meaning that names have to be matched up carefully to avoid incorrect deliveries – which are themselves problematic from the perspective of data protection law. This takes up a lot of time and can involve a lot of work, particularly on the part of postmen and postwomen who are not familiar with the building in question.

To minimise the rate of incorrect deliveries and make life easier for postmen and postwomen, Deutsche Post AG launched a system – initially in the form of a pilot scheme – that involved recording the position of letterboxes within a bank (e.g. fourth row down, third along) before matching this position up to the names and address of the people living there. This information can then be used as the basis for “carrier sequence sorting”, which means that the letters in the postman or postwoman’s bag are already in the same sequence as the individual letterboxes in each bank of letterboxes.

The legal basis for data processing in this connection is, first and foremost, the legitimate

interests of the postal service provider. Natural persons were informed in writing that their “letterbox data” had been recorded in keeping with the duty to provide information pursuant to the GDPR. Data subjects are entitled to object to the processing of their data if they do not consent to it.

Deutsche Post AG presented the project to me at an early stage so that I could highlight some areas for improvement from the outset. For example, I was able to ensure that the correct legal basis was selected and to influence key aspects of the technical and organisational measures, the way in which information was provided to data subjects and the handling of data subjects’ rights. My suggestions were welcomed by Deutsche Post AG and implemented before the pilot scheme was rolled out on a wider basis.

8.9 Fining methodology issued by the data protection authorities

The DSK has published a joint fining methodology to be applied in proceedings against companies. According to this methodology, it should be ensured that fines are effective, proportionate and dissuasive by setting them firstly according to the gravity of the infringement and secondly according to the size of the company. The German data protection authorities are also working together with the European supervisory authorities on EU-wide guidelines.

New era ushered in by the GDPR

For the first time ever, the GDPR provides for uniform remedial powers throughout the EU. At the same time, the power to impose monetary fines is incorporated into a larger system of differentiated corrective actions that can be taken by the data protection authorities for the purpose of enforcing the legislation, ranging from simple warnings and reprimands through to orders and fines. The data protection authorities are granted the discretion to choose between the various remedial measures or to apply several on a cumulative basis.

Pursuant to Article 58(2)(i) in conjunction with Article 83(4) to (6) GDPR, formal infringements are subject to administrative fines of up to EUR 10,000,000 or 2% of the total worldwide annual turnover of the preceding fiscal year, and material infringements are subject to administrative fines of up to EUR 20,000,000 or 4% of the total worldwide annual turnover of the preceding fiscal year. European indirect joint liability within a group applies, which is a shift away from (and goes further

than) the previous tradition of German law. The EU has therefore assigned the same significance and scope to infringements of European data protection law as to infringements of European competition law.

European principles and guidelines

In the interests of effective implementation practice, the European legislator has added three sanctioning principles to the enforcement programme for data protection authorities that are familiar from competition law: effectiveness, proportionality and dissuasion. In addition, Article 83(2) GDPR sets out a number of discretionary factors to be reviewed by the data protection authorities when deciding whether to impose a fine and how much the fine should be.

With a view to guaranteeing uniform implementation throughout the EU, Article 70(1)(k) GDPR assigns the EDPB the task of drawing up guidelines for the setting of administrative fines pursuant to Article 83 GDPR on the basis of these principles. The EDPB made its first move in this direction at its first plenary meeting on 25 May 2018, when it endorsed the guidelines on the application and setting of administrative fines which its predecessor, the Article 29 Working Party, had already adopted in preparation for the GDPR. These guidelines, published on 3 October 2017 (available at: <http://www.bfdi.bund.de/guidelines>), start by establishing a common understanding of the provisions of Article 83 GDPR and outlining a consistent approach to the principles that apply when setting administrative fines. For example, it was clarified that the notion of an “undertaking” should be defined as provided for by Articles 101 and 102 TFEU in accordance with Recital 150 GDPR. An undertaking must therefore be understood to be the economic unit which engages in commercial/economic activities, regardless of the legal person and the nature of its funding. It can consist of several natural or legal persons, which represents a significant departure from the previous tradition of German law.

The Article 29 Working Party stated that the methodology to be followed when setting fines would be clarified by the EDPB in later guidelines; these are currently being debated.

German fining methodology

With a view to ensuring uniform implementation within Germany during the transitional period until the relevant guidelines are adopted, on 16 October 2019, the DSK published a joint fining methodology

to be applied in proceedings against companies (available at: www.bfdi.bund.de/beschlusspositionspapiere). This methodology does not have binding effect in “cross-border cases”, where cooperation with the European supervisory authorities – which are not subject to the methodology – is required, and so its scope is explicitly restricted to “domestic” cases.

This methodology also marks an attempt by data protection authorities to bring their supervisory practice into line with a legislative decision that requires higher fines than the previous legal situation, while taking particular account of the special economic situation of microenterprises and small and medium-sized enterprises (SMEs) in order to avoid subjecting them to the same level of fines as large undertakings. The methodology does not apply to associations and natural persons that are not engaged in economic activities.

The methodology outlines a five-stage procedure for the setting of fines in proceedings against companies. Initially, in Stages 1 to 3, a basic amount is calculated according to the size of the undertaking. Secondly, in Stages 4 and 5, the amount is adjusted depending on the offence, the perpetrator and other circumstances of the individual case. Considerations specific to the undertaking may also be taken into account during the last stage, for example the risk of bankruptcy, a high turnover or a low profit margin, provided that the level of turnover is not dependent on a data-driven business model.

All the discretionary factors pursuant to Article 83(2) GDPR must be taken into account by the data protection authorities during this stage-by-stage process. Ultimately, and while applying all the factors referred to in Article 83(2) GDPR, the methodology therefore combines two key considerations: the gravity of the infringement and the size of the undertaking, ensuring that fines are appropriate to the actual infringement and the undertaking in question. This combination guarantees compliance with the sanctioning principles of effectiveness, proportionality and dissuasion that have been prescribed by the legislator. The data protection authorities will carry out regular evaluations to determine whether the methodology does, in fact, implement these principles in practice, or whether it should be improved to meet the EU’s requirement of effectiveness (*effet utile*).

Conclusion and outlook

The DSK’s joint fining methodology to be applied in

proceedings against companies represents an example of how uniform implementation and enforcement of data protection law is possible in a federal supervisory system. It is a vital first step along the road towards a common and uniform strategy for enforcement of the law, but further steps urgently need to be taken. The need for a common law enforcement strategy is particularly pressing in view of the other potential remedial powers which are already being implemented instead of or in addition to fines, and which need to be implemented consistently.

German undertakings, data protection authorities and courts must bring their way of working into line with the new European sanctioning regime, and Germany's fining methodology is a first move in this direction. European guidelines should be adopted as soon as possible in the interests of EU-wide harmonisation.

8.10 Green light for accreditation

The GDPR introduces the concept of data protection certification as a means of proving compliance with its provisions. To ensure that these certifications do, in fact, guarantee the stated level of quality, Article 43 GDPR provides for the accreditation of certification bodies.

The GDPR provides the option of voluntary audits of compliance with its provisions, resulting in either certification or a European Data Protection Seal. It lays down a basic legal framework for this purpose in Articles 42 and 43. These provisions are intended to increase transparency and improve compliance with the provisions of data protection law. At the same time, however, bodies may issue certifications pursuant to Article 42 GDPR only if their suitability to conduct certification procedures has been checked and they have been formally accredited. This procedure serves as a key basis for establishing a heightened and common level of data protection throughout the EU. The provisions of the GDPR merely provide a general overview of the accreditation procedure, and the Member States are responsible for fleshing out the details. This is intended to provide leeway for adjustments to specific national circumstances. Germany made use of this option in Section 39 BDSG.

National implementation

With a view to ensuring that the quality of certification is as high as possible, Article 43 GDPR provides for the preliminary accreditation of certification bodies by way of a conformity assessment. This has opened up a whole new area of

work for the data protection supervisory authorities, since they play a key role in this accreditation process. Pursuant to Section 39 BDSG, the competent data protection supervisory authority, on the basis of accreditation by Deutsche Akkreditierungsstelle GmbH (DAkkS), is responsible for deciding whether a party can act as a certification body. Detailed provisions regulating this procedure can be found in the [German] Accreditation Body Act (*Akkreditierungsstellengesetz, AkkStelleG*). For example, the latter states that the data protection supervisory authority responsible for granting powers should always handle the relevant accreditation procedure jointly with DAkkS. The accreditation process for data protection certification is divided into six phases:

1. application phase – programme appraisal
2. programme appraisal and approval of criteria
3. application phase for accreditation/granting of powers
4. assessment phase
5. accreditation phase/granting of powers
6. supervision phase

The data protection supervisory authorities of the Federal Government and the *Länder* are closely involved in the work ongoing within national committees with a view to transposing the GDPR provisions on the national accreditation procedure. For example, they have developed a concept containing requirements that apply alongside DIN EN ISO/IEC 17065, as explicitly demanded by the GDPR. This concept includes in-depth examinations of topics relating to the conformity assessment, and is supplemented by the position paper published by the supervisory authorities on "Data protection principles to be considered in relation to the requirements that apply to the structures, resources and processes or the management systems of bodies to be accredited" (<https://www.datenschutzkonferenz-online.de/anwendungshinweise.html>). The DSK is currently in the process of making final amendments to this document, which will then need to complete the necessary approval processes at European level.

In addition, an agreement was also reached at national level between the data protection supervisory authorities of the Federal Government and *Länder* and DAkkS regarding accreditation tasks, setting out clear rules on jurisdiction and responsibilities and ultimately clarifying the

provisions of the Federal Data Protection Act and the Accreditation Body Act. This is merely one example illustrating the scope and level of detail in which this new accreditation task must be regulated and agreed at national level to comply with the provisions of data protection law. Negotiations between the various stakeholders took longer than originally expected, as did the process of fleshing out the individual procedural stages. Modifications will also need to be made at European level, but empirical values are currently lacking.

The EDPB

Over the past year, the EDPB published guidelines highlighting the main points to be taken into consideration during the accreditation procedure (the guidelines, published on 14 December 2018, can be accessed at:

<http://www.bfdi.bund.de/guidelines>). In parallel, committees at EU level are also working out the details of corresponding procedures for implementing accreditation and certification mechanisms within the EDPB structures.

For example, in future, the EDPB must guarantee that it can issue opinions on drafts by the supervisory authorities of the Member States relating to the adoption of requirements for the accreditation of certification bodies pursuant to Article 43(3) GDPR or the approval of the certification criteria referred to in Article 42(5) GDPR (Article 64(1)(c) GDPR). In addition, pursuant to Article 42(5) GDPR (Article 70(1)(o) GDPR), EU-wide certification criteria must be approved as a basis for a European Data Protection Seal. Consistent procedures at EU level are an essential prerequisite for ensuring that the Member States can commence activities relating to national and EU-wide certification. Most of the procedural stages have now been agreed upon within the EDPB, and the further details will be defined and approved in the further course of work.

First accreditation procedures to be launched in 2020

Accreditation is a new task that will entail a great many fresh challenges for all those involved. In-depth discussions have been held at both European and national level on the details of the relevant procedures and processes. The first accreditation procedures will be launched in 2020.

My goal in this respect was – and still is – to create a robust, transparent and reliable accreditation procedure with a view to making data protection certifications more credible, since this is a vital

prerequisite for ensuring that they genuinely boost confidence and create added value.

In future, the option of purchasing products and services with data protection certifications will make it easier for companies – in particular smaller companies – to be confident that they are acting in line with data protection requirements.

8.11 Federal IT Consolidation Project

The Federal IT Consolidation Project (*IT-Konsolidierung Bund*) is aimed at safeguarding the Federal Government's capacity to work digitally over the next few years and at guaranteeing the efficiency of its operations. Compliance with the provisions of data protection law is a fundamental requirement in this respect, and I therefore offer advice to the individual subprojects of the Federal IT Consolidation Project.

The Federal Cabinet approved the reorganisation of the Federal IT Consolidation Project on 6 November 2019. In future, the German Federal Ministry of Finance (*Bundesministerium der Finanzen*, BMF) will be responsible for the consolidation of operations, while the BMI will remain responsible for the consolidation of services. Further changes within the Association of Service Providers (*Dienstleisterverbund*) led to delays in many of the subprojects being implemented by the Federal IT Consolidation Project.

As was previously the case, the advice I provided focused chiefly on Subproject 6: "Consolidation of Services". This Subproject incorporates many different measures such as the "Federal Client", the "Federal Cloud", "Identity and Access Management" and the "multi-functional electronic ID card". The changes taking place within the Association of Service Providers meant that work needed to be halted on the "Identity and Access Management" measure, which in turn meant delays for the "Federal Cloud" and "Federal Client" measures.

The "Federal Cloud" is defined as a standardised scalable platform for basic, cross-cutting and specialised IT procedures within the Federal Government. It is operated as a private cloud by the Federal Government's data centres, and already provides services for a number of pilot authorities. The most pressing task at present is to gain approval for the processing of documents with the status of "classified, for official use only" in the Federal Cloud. Going forward, I will continue to work on these topics and to provide advice on the portfolio of

services operated in the Federal Cloud.

The “Federal Client” measure involves making available – by the end of 2025 and throughout Germany – uniform workstations that use a standardised operating system as well as basic and horizontal functions such as e-mail and word processing applications. The Federal Client is currently being tested by the Federal Information Technology Centre (*ITZ Bund*). I will provide the necessary support for these tests by responding to any questions relating to data protection.

A great deal of collaborative work took place within the relevant committees (for example in relation to the Architecture Guidelines Committee) with a view to providing long-term support for project managers taking strategic decisions in connection with the Federal IT Consolidation Project. Information is regularly exchanged with the overall project leads, and BfDI representatives attend departmental workshops with a view to asking and answering questions about data protection.

In conclusion, the level of cooperation with all stakeholders, including the Federal Government's IT Service Provider, is good. This means that I can perform my task of monitoring compliance by the Federal IT Consolidation Project with data protection requirements and provide advice to all those involved.

8.12 Data protection and Windows 10

The forwarding of telemetry data from Windows 10 operating systems to Microsoft raises problems under data protection law for all of the bodies under the BfDI's oversight. Particularly in the field of public administration, it is therefore important to strengthen digital sovereignty to avoid dependence on individual manufacturers of hardware and software platforms.

In late 2018, the BSI published the outcomes of its SiSyPHuS study on Windows 10. The main focus of this study was to determine the extent to which “telemetry data” were forwarded by the operating system to Microsoft via the Internet.

At the start of the year, I was also forwarded the outcomes of an investigation into the links between existing Windows 10 clients within the Federal Administration's networks and Microsoft's telemetry servers, which revealed that significant volumes of data had been transferred during the period between October 2018 and January 2019.

These telemetry data are processed using data

collected in the form of system events such as button presses or print job requests. These system events are assigned to user identifiers that make it possible for Microsoft to (re)identify an individual user on an individual device together with the relevant use pattern. This tagging (and therefore the link to the individual) happens across the board, i.e. in every version of Windows 10 and at every telemetry level (a setting that determines the amount of data sent). The telemetry level is a key factor determining which of these tagged events are collected using “measurement points” and sent to Microsoft. There is one other important factor, however: user behaviour. Telemetry services are controlled by a configuration file that is regularly updated by Microsoft so that the measurement points and the content of the telemetry data can be adjusted to user behaviour.

The “customisation” of telemetry services to each individual system renders it impossible to make generalised statements about the telemetry data that are collected and sent to the manufacturer. A test carried out on an individual system is only ever a single snapshot. The scope of the telemetry data that are sent may change from one moment to the next, depending on how the user behaves. It is also impossible to “measure” the secondary telemetry services by means of which Microsoft accesses a Windows 10 system and execute files and functions, e.g. by reading the main memory. It is not yet clear which user behaviour triggers changes in the telemetry services.

This in turn affects the way in which use of Windows 10 is assessed from the perspective of data protection law. I am actively involved in the working group set up by the DSK with a view to ensuring the uniformity of such an assessment. The stated intention of this group is to issue an opinion on Windows 10 from the perspective of data protection law, with the primary aim of creating legal certainty for users.

Although the final opinion was not yet available by the editorial deadline for this document owing to the aforementioned technical complexity of the procedures involved in processing telemetry data, there is no question about the fact that these data processing operations are problematic from the viewpoint of data protection law. The most contentious issue relates to the legal basis for the processing of personal data by Microsoft in the case at hand.

In my opinion, the purposes of telemetry data processing cited by Microsoft in its privacy statement could also be achieved using non-personal

data. This would mean that maintaining a link between the data and the individual data subject would not generally be necessary to safeguard Microsoft's interests. I therefore proposed to Microsoft that it should remove the link with the individual data subject by using random numbers, for example, instead of user identifiers; this is an alternative that has already been opted for by several providers of comparable products. Microsoft has agreed to review this proposal.

Separating the operating system features from the Internet appears to be one way of running Windows 10 in a manner that complies with data protection principles, and this is solution that will be used in future for the Federal Administration's Federal Client. This is feasible only if Windows 10 is operated locally on a workstation, however. If Microsoft were to move to offering Windows solely as a cloud service (as per their stated plans), this solution would no longer be possible.

On 7 November 2019, the DSK working group published guidance for all those who wish to process personal and non-personal data using Windows 10. This guidance takes the form of a series of checks, and is available at <https://www.bfdi.bund.de/beschluesse-positionspapiere>.

During a Windows 10 test carried out in December by the Bavarian State Office for Data Protection Supervision (*Bayerisches Landesamt für Datenschutzaufsicht*) together with Microsoft in the presence of BfDI representatives, user activity was generated on a system using a script (Invoke-UserSimulator) and network traffic was logged. No evidence was found that telemetry data were being sent. This test represented only a snapshot of

Windows 10, however, since the scope of the telemetry data sent can change from one moment to the next depending on user behaviour. It is therefore necessary to await the outcomes of further investigations by the BSI, which were not yet available by the editorial deadline for this document. This is the only way to ascertain whether Microsoft has followed through on its promise to modify Windows 10 in such a way as to ensure that only the data required for operational purposes are sent, and all the data sent can be reviewed by the user.

I will, in any event, remain in discussions with Microsoft in the hope of finding a solution that is acceptable to all sides; this year alone, I have met several times with Microsoft representatives.

Strengthening of digital sovereignty

The problems faced in connection with Windows 10 demonstrate the importance of choice when selecting hardware and software platforms. I therefore welcome the Federal Government's Digital Sovereignty Initiative. Under this project, the Federal Government, the *Länder* and the municipalities will join forces to reduce their level of dependence on individual manufacturers; this will be an ongoing process rather than a one-off event. Action of this kind is the only way to achieve a sustainable product procurement process that meets the necessary standards in terms of security and data protection. Until this goal has been achieved, efforts must be undertaken to decouple specialist applications from hardware and software platforms, for example by ensuring that they use standard database interfaces. I will try to gain a wider audience for this topic within the relevant bodies.

9. Internal developments within the BfDI

9.1 Staffing changes and internal organisation

Recruiting new staff on the basis of budgetary approvals allows the BfDI to provide more advice, carry out more controls and step up its cooperation efforts. Internal structural reorganisations proved necessary in view of the constant rise in the amount of work and the associated increase in staffing levels.

The staffing situation has improved considerably since the BfDI became an independent body on 1 January 2016. By 2019, I was able to increase staffing levels to a total of 253.5 FTEs. The additional staff recruited made it possible for the BfDI not only to set up the necessary official structures, but also to perform the additional tasks it had been assigned, particularly in connection with the GDPR (e.g. Legal Department, Fines Department, Single Contact Point, data protection supervision of the fiscal authorities, municipal tax offices and job centres) and to respond to certain procedural changes (e.g. formal complaint procedure, appointment of a representative to the EDPB).

The budgetary legislator has promised an additional 67 FTEs for 2020. Many of the new recruits will be involved in data protection supervision of the security authorities, with a view to performing the compensatory function called for by the Federal Constitutional Court. The BfDI was also granted 4.4 FTEs by the BNetzA pursuant to Section 50 of the [German] Federal Budget Code (*Bundeshaushaltsordnung*, BHO). This follows from the transfer of competences under data protection law from the BNetzA to the BfDI, as reported in No. 15.1.4 of the 27th Activity Report.

I very much welcome these positive ongoing developments, since they make it possible for the BfDI to provide more advice to bodies under its oversight, to the Bundestag and to the public, to carry out controls to a higher standard and to earmark resources for increased international

cooperation on data protection and further harmonisation in this area.

The rapid increase in staffing levels and new tasks made it necessary to carry out a structural reorganisation within the BfDI, which was completed by 1 August 2019. Two new departmental groups were established, and the organisational units that had previously been managed as working groups were converted into separate departments.

All administrative tasks for the BfDI as a whole, including HR-related matters, organisation, budget, internal services, procurement and ICT support, are bundled within the “Central Tasks” Departmental Group, which is split into four departments.

The steady increase in tasks in the field of security also made it necessary to set up a separate “Police and Intelligence Services” Departmental Group, which is split into four specialist departments. The security authorities will only expand in future, and the effective data protection supervision required by the Federal Constitutional Court as a compensatory function means that our tasks in this area will increase correspondingly, creating a need for the performance of more tasks and further staffing increases.

In my opinion, the reorganised BfDI is in a good position to carry out its data protection supervision tasks effectively, both now and in the future.

9.2 Public outreach work

Public demand for information on the GDPR continued to be high in 2019. I also launched a new corporate design this year. The shift away from the Federal Government’s design that had previously been used was aimed at making my independent status immediately obvious.

Corporate design

The publication of my 27th Activity Report on Data Protection marked the launch of a new corporate

design for the BfDI. The aim of this redesign was to make my independent status more immediately obvious. During the reporting period, it was possible to complete the transition to the new design for most of my external communications materials.

Remaining stocks of printed publications were used up before reprints were ordered. As well as the reprinting of a number of flyers and brochures, a website relaunch is scheduled and likely to be completed in 2020.

Events

Over the course of the past year, I organised a symposium in Berlin under the heading “Chances and risks for the privacy-friendly use of artificial intelligence”. The event served as a forum for discussion among over 150 attendees, who exchanged views on data protection and artificial intelligence. I was able to welcome over 150 participants to this event and provide them with a platform for discussing data protection and artificial intelligence. Together with the European Data Protection Supervisor, I also organised a panel discussion attended by over 300 guests on the challenges facing data protection and competitiveness in the digital age. Similar events are also planned for the future.

Visitor groups

My co-workers welcomed a total of 15 groups of up to 50 visitors in 2019. Twelve of these events were arranged by members of the Bundestag.

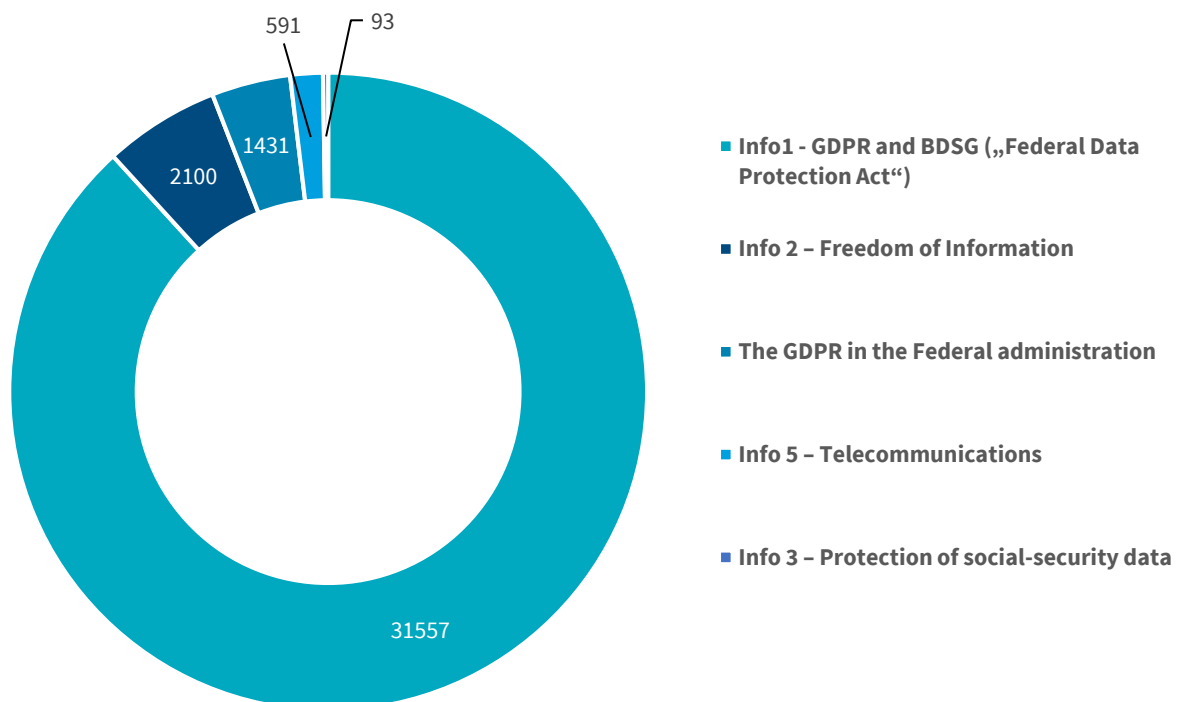
Information material

An important part of my public outreach work relates to the publication of flyers and brochures. The information brochures are targeted at readers looking for a deep dive into a particular topic. They contain not only insights into certain legal issues, but also reproductions of the relevant legislative provisions. The flyers, which are shorter and more reader-friendly, are designed especially with citizens in mind. They contain brief overviews and clear recommendations on data protection.

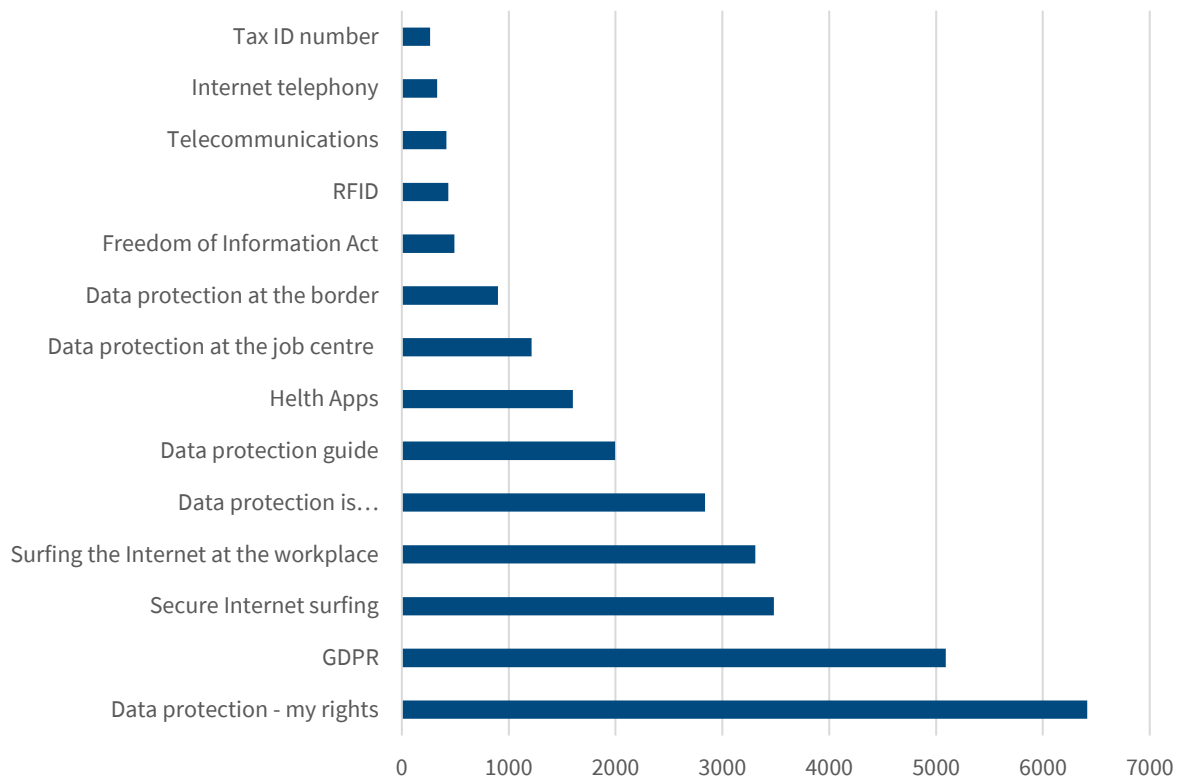
All of our information brochures are very popular (see diagrams).

All current publications can be ordered at www.bfdi.bund.de/informationmaterial or downloaded in PDF format.

Brochures submitted



Flyers submitted



9.3 The BfDI's work in figures

Disregarding my tasks as a supervisory and control authority under data protection law, the bulk of my activities involve providing advice to citizens, the German Bundestag and the data-processing institutions that fall under my jurisdiction. There continued to be a huge demand for the BfDI's expertise during the first full calendar year of application of the GDPR.

Complaints and general queries

I received many complaints about data breaches from citizens. Enquiries are regarded as complaints if data subjects believe that their rights have been infringed as a result of the collection, processing or use of their personal data. The right to lodge a complaint is enshrined in special legislative acts as well as in the GDPR.

In 2019, I received 3,118 complaints pursuant to Article 77 GDPR (Right to lodge a complaint with a supervisory authority). In addition, I recorded 44 complaints pursuant to Section 60 BDSG (Referral to the Federal Commissioner for Data Protection and

Freedom of Information) and 44 submissions relating

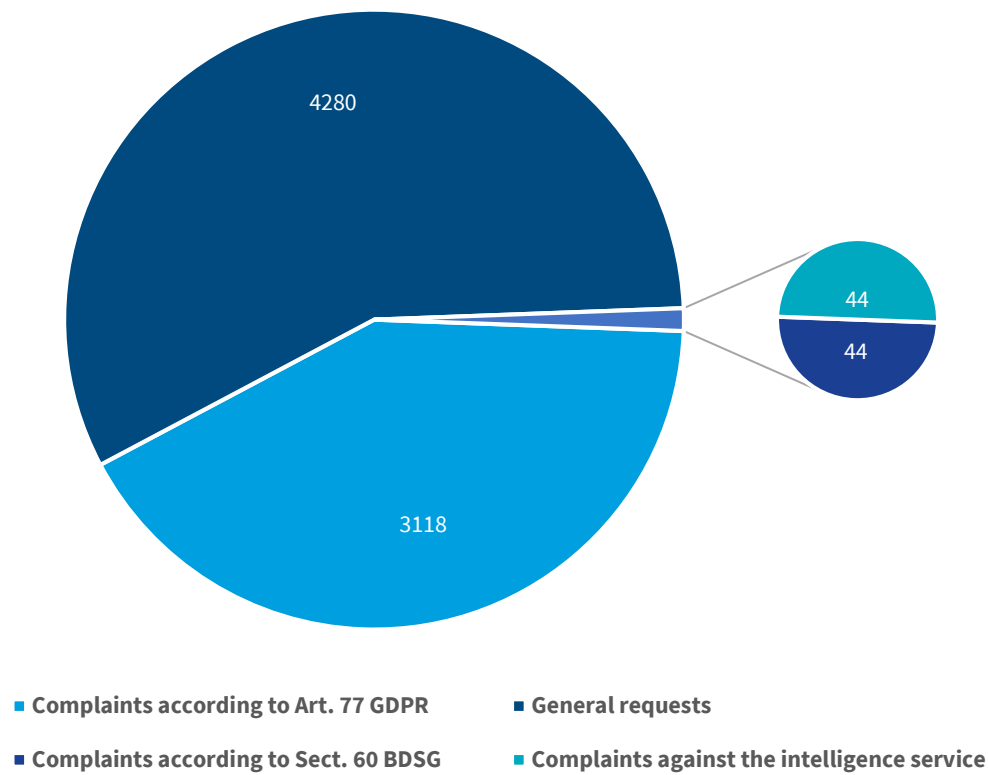
to intelligence services. I also received three complaints pursuant to Article 89 GDPR.

Advice and controls

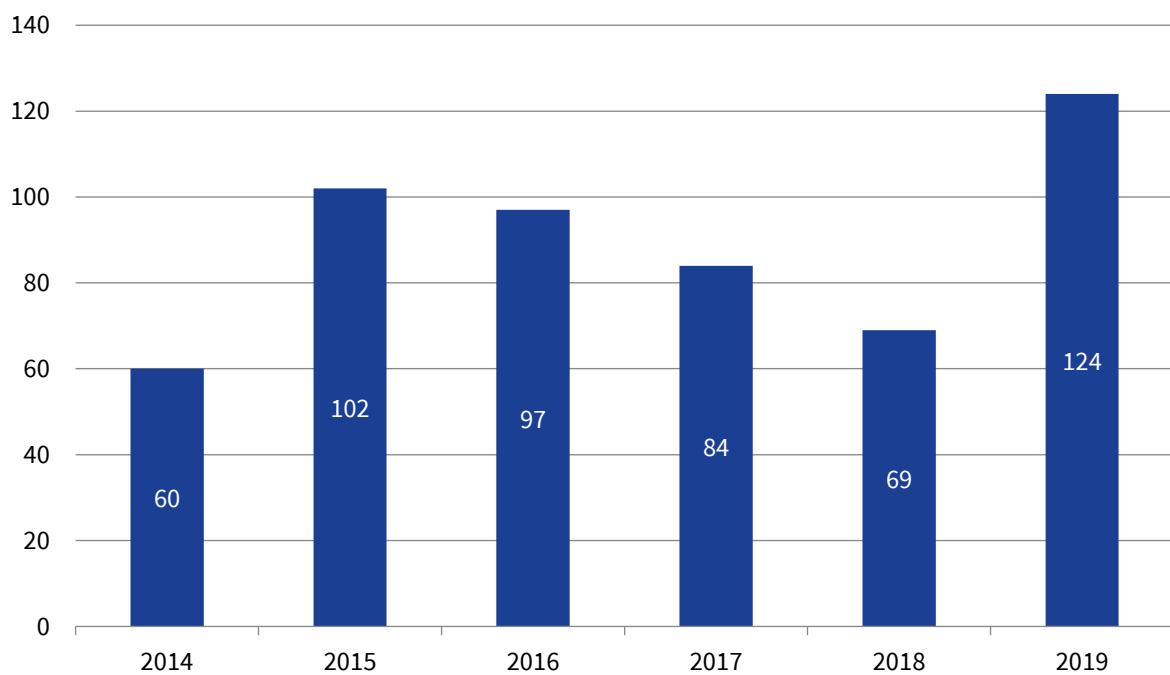
An important part of my work involves providing advice to controllers and data subjects. In 2019, the BfDI received 4,280 written general enquiries from citizens. I also provided advice by telephone in a further 6,939 cases.

I carried out in-person visits to a total of 124 data-processing institutions that fall under my jurisdiction. Of these visits, 51 were carried out purely for the purpose of providing information and advice. Controls under data protection law were also carried out during 73 of the visits. In addition to these in-person visits, my co-workers also regularly provided advice to the institutions that fall under my jurisdiction on matters relating to data protection law, both in writing and by telephone.

Complaints and requests



Visits for the purpose of providing information, advice and performing controls



Data breach notifications

All public and non-public bodies must notify data breaches to the competent supervisory authority. During the reporting period, the BfDI received almost 15,000 notifications of this kind.

Data breach notifications	2019
Article 33 GDPR	14,649
Section 65 BDSG	0
Section 109a (1) TKG	40

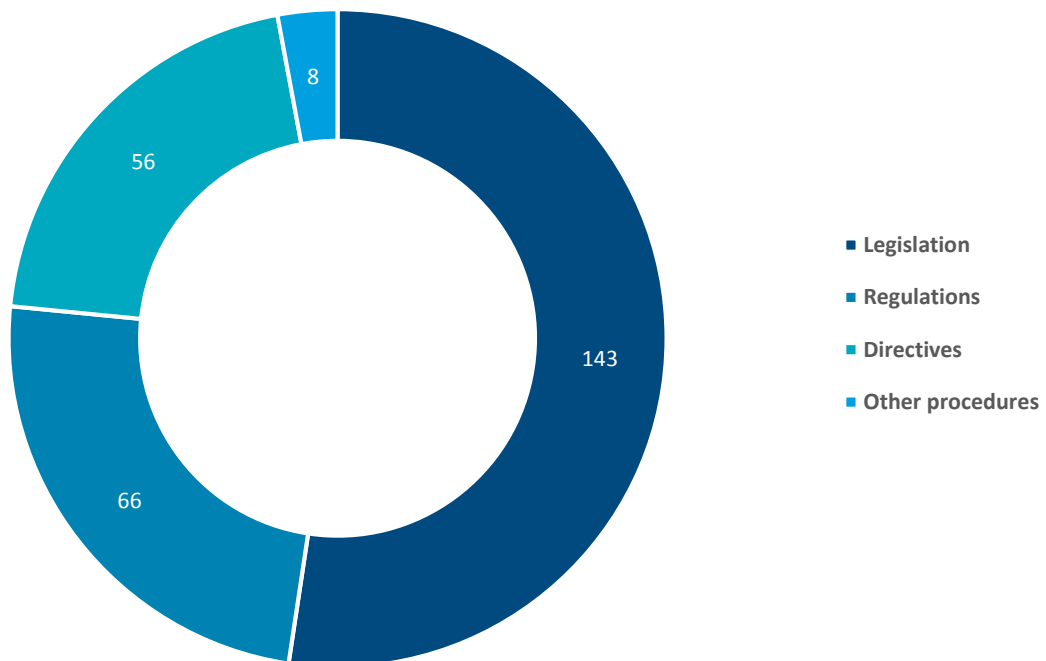
Remedial measures

During the reporting period, I issued six warnings pursuant to Article 58 GDPR and lodged eight complaints pursuant to Section 16 BDSG. I also imposed two fines pursuant to Article 83 GDPR.

Formal support for legislative projects

Pursuant to Section 45 GGO, the competent federal ministry must involve me at an early stage in the process of drafting legislative bills that fall under my remit. During the reporting period, I examined and monitored 143 legislative procedures, 66 regulatory procedures and 56 sets of guidelines as well as eight other legislative initiatives that required my involvement pursuant to Section 21 GGO.

Involvements according to Sect. 21 of the Joint Rules of Procedure of the Federal Ministries



Other procedures involving the BfDI

I also issued opinions on 32 file orders, three sets of proceedings before the Federal Constitutional Court and five EU legislative acts. In addition, I was able to contribute my expertise during five public hearings before the German Bundestag.

Miscellaneous

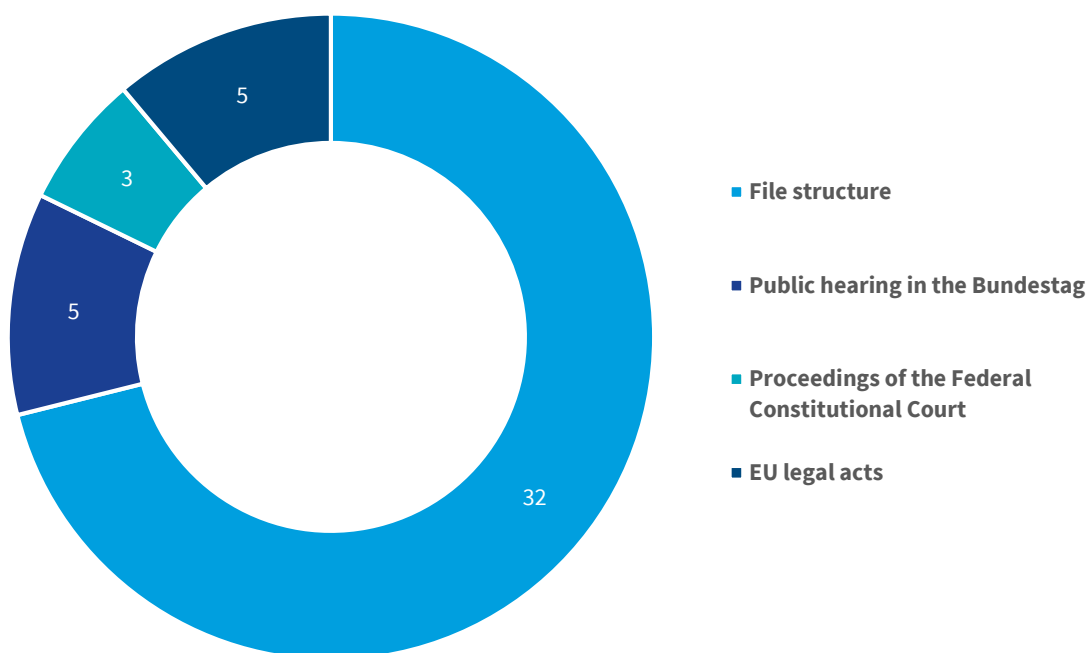
Over the past year, 25 appeals were lodged against decisions taken by the BfDI. During the subsequent

proceedings before courts of first instance, decisions were handed down in favour of my office in three cases, although the decisions have not yet become final. In three other cases, the appeals that were initially lodged were retracted by the opposing party upon request by the courts. The remaining cases (19 in total) were still pending before the courts at the end of the reporting period.

Cross-reference:

10.2 Statistical overview of proceedings before the Single Contact Point.

Other procedures with the involvement of the BfDI



10. BfDI as the Single Contact Point

10.1 Cooperation between the national supervisory authorities on European topics

Pursuant to Article 51(3) in conjunction with Recital 119 GDPR, Germany, as a Member State with several supervisory authorities, must designate a single contact point for the effective participation of all German supervisory authorities and smooth cooperation with the other European bodies on procedures under the GDPR. The operational processes agreed at the level of the EDPB are adapted by the Single Contact Point to the federal German system.

Day-to-day operations within the Single Contact Point involve coordinating the flow of information between the European supervisory authorities and the EDPB on the one hand, and the supervisory authorities of the Federal Government and the *Länder* on the other.

In addition, a comparatively large proportion of the work carried out by the Single Contact Point is proactive in nature. It involves adapting the processes agreed at EDPB level in relation to European cooperation to the realities of federally structured cooperation between the supervisory authorities of Germany's Federal Government and *Länder*. Although the task of data protection supervision is divided between different levels of the federal structure, it is essential for cooperation with the European supervisory authorities and the EDPB to run quickly and smoothly.

The GDPR merely lays down the broad strokes of cooperation at EU level, and tasks the EDPB with deciding on the further details. The EDPB has made ample use of this opportunity with the aim of making the statutory procedures easier to implement. Nevertheless, the Member States – including Germany – remain responsible for domestic administrative arrangements. The two examples outlined below illustrate the types of interactions that take

place between cooperation processes at European and national level.

In the event that supervisory authorities wish to approve BCRs, they must apply for an opinion from the EDPB (Article 64(1)(f) GDPR). The highly formal procedure outlined in the GDPR involves short deadlines for the adoption of decisions. An application for an opinion from the EDPB is typically preceded by several years of intense collaboration between the company in question, the competent supervisory authority (generally the supervisory authority responsible for the country in which the company has its EU headquarters) and often two other supervisory authorities (co-examiners).

Complex and iterative work of this nature cannot easily be translated to the formal proceedings before the EDPB that are described in the GDPR. Steps have therefore been taken to introduce an informal preliminary procedure between the supervisory authorities, which takes place prior to the application proper. All of the European supervisory authorities are involved in BCR procedures of this kind, ensuring that any remarks or comments by the individual supervisory authorities are taken into account before the BCRs in question are referred to the EDPB. The Single Contact Point is responsible for coordinating collaboration between all the German supervisory authorities at national level with a view to reaching a consensus opinion within Germany on the individual BCRs and voicing this opinion at national level. The Single Contact Point has sketched out an operational procedure for this purpose that is currently being negotiated with the supervisory authorities of the Federal Government and the *Länder*.

The GDPR is reticent on the subject of the adoption of resolutions by the EDPB, and so the EDPB has adopted supplementary provisions in its Rules of Procedure. These Rules of Procedure also provide for a written voting procedure as a way of taking decisions outside meetings. A deadline of one week is typically set for a written voting procedure. Within

this short deadline, the Single Contact Point must inform the 18 supervisory authorities of the Federal Government and the *Länder* about the voting procedure and initiate the relevant national decision-making processes. Once again, the general principle of voting applies, namely that Germany has only one vote within the EDPB in spite of the fact that it has several different supervisory authorities. If no agreement can be reached, a common position must be agreed upon within the voting period as an outcome of “contentious” proceedings pursuant to Section 18 (2) BDSG, with a view to ensuring that Germany can vote in a timely manner within the EDPB. With this in mind, the Single Contact Point has already put in place a preliminary operational procedure aimed at ensuring that the voice of the German data protection supervisory authorities can be heard at European level.

Given the ever-evolving nature of European cooperation, the development (and further development) of processes remains an ongoing task for the Single Contact Point

10.2 Statistical overview of cooperation and cohesion procedures at European level

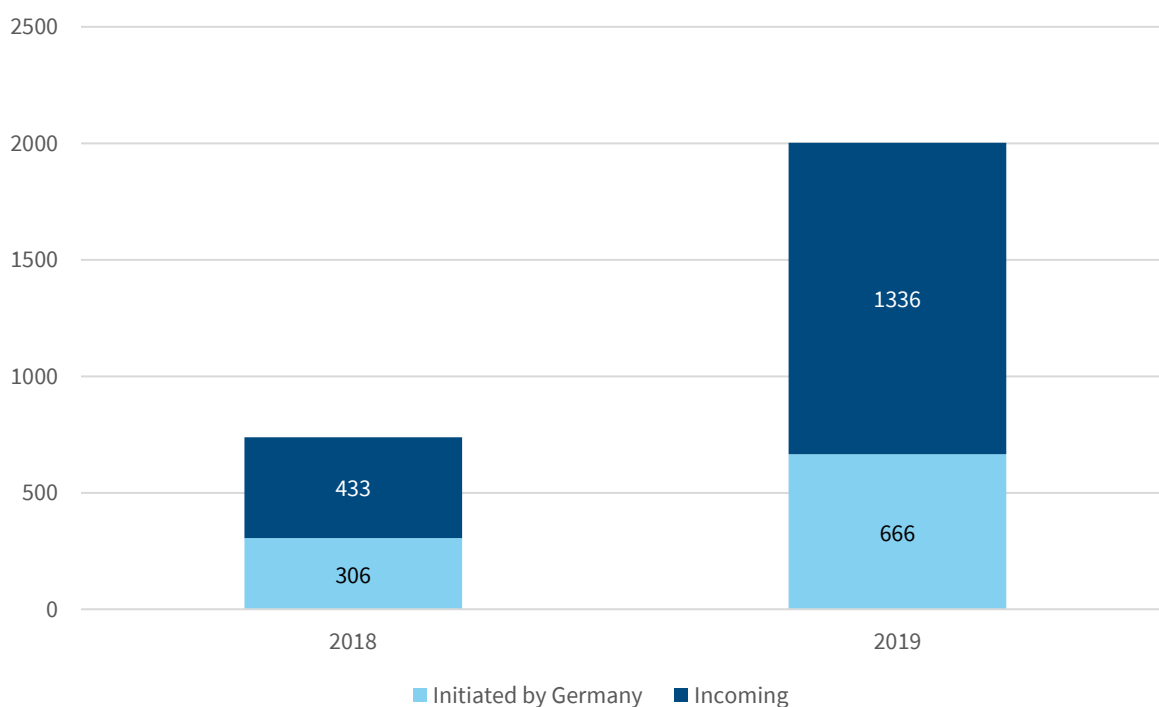
from the perspective of the Single Contact Point

The Single Contact Point continues to serve a vital role as a connecting link from and to Europe. It coordinates the flow of information between the European supervisory authorities and the EDPB on the one hand, and between the supervisory authorities of the Federal Government and the *Länder* on the other.

The scale of this task increased considerably over the reporting period compared to the previous year, as illustrated by the rise in the number of individual procedures recorded

within the Internal Market Information (IMI) system. Both the total number of procedures and the number of procedures with German involvement more than doubled between 2018 and 2019. The statistics shown overleaf make it clear that the supervisory authorities in Europe are working together more effectively than ever before. In 2018, the main focus was still on identifying the lead supervisory authorities/other supervisory authorities concerned (Article 56 procedure), but attention is now shifting to the processing of actual cases. The supervisory authorities exchange information on the processing of cases via informal

Procedures with the involvement of Germany



consultations pursuant to Article 60 GDPR and via

mutual assistance procedures pursuant to Article 61

GDPR. If the intention is to adopt a decision (an administrative act under German law), the decision is presented in advance to the other supervisory authorities concerned as a draft for their opinion (Article 60 procedure, draft decision, revised draft decision). After its adoption, the decision is notified to the other supervisory authorities (Article 60 procedure, final decision). The number of final decisions adopted is not the same as the overall number of procedures that are completed, since many procedures can be terminated informally because there is no further need for action. As with cooperation on the processing of cases, work within the EDPB is increasingly settling into an established routine. There was a drop in the number of opinions obtained from the EDPB pursuant to Article 64 GDPR (31 procedures between 25 May 2018 and 31 December 2018 compared to 30 during the whole of 2019), which can be attributed to the fact that the mandatory tasks provided for in the GDPR

(e.g. adoption of a list of processing operations for which a data protection impact assessment must be carried out) have, to a large extent, already been carried out.

Increasingly, however, the EDPB is carrying out tasks on a voluntary and own-initiative basis, particularly in respect of opinions and guidelines (Article 70 GDPR), in order to emphasise certain aspects of data protection law (see No. 3.2.1).

Overall, the need for coordination by the Single Contact Point has stepped up, as evidenced by the number of internal consultations within the IMI system, which rose from 43 in 2018 to 62 in 2019. Internal consultations are initiated by the Single Contact Point and serve as a basis for preparing a uniform response by Germany to the EDPB or other supervisory authorities involved in the IMI system.

Cross-references:

3.2 EDPB

Cooperation procedures during the reporting year

Procedure	Total	Initiated by German supervisory authorities	Comments
Article 56 – Identification of LSA and CSA	906	261	
Article 56 – Local case request	5	3	Only procedures involving Germany
Article 60 – Draft decision	95	20	Only procedures involving Germany
Article 60 – Revised draft decision	9	3	Only procedures involving Germany
Article 60 – Final decision	81	11	Only procedures involving Germany
Article 60 – Informal consultation	188	29	Only procedures involving Germany
Article 61 – Mutual assistance	25	17	Only requests from and to Germany
Article 61 – Voluntary assistance	601	260	Only requests from and to Germany
Article 64 – Opinion by the EDPB	30	0	Received by Single Contact Point, distributed via internal consultation, includes only published procedures
Article 64 – Final EDPB opinion	0	0	Received by Single Contact Point, distributed via internal consultation,
Internal consultation		62	Initiated centrally by Single Contact Point for national coordination
Total	2,002	666	

Keyword directory

The reference is the number of the article in which the term is used.

- Access system 7.1
- Accreditation 3.1, 3.2, 4.1, 8.10
- Activity Report on Data Protection 9.1
- Adequacy decision 8.1.1
- Anonymisation 4.6, 5.3.3
- Anti-terror file (Anti-Terror-Datei, ATD) 2.2, 6.7.1
- Approach , risk-based 4.4, 4.6
- Article 29 Working Party 8.9
- Artificial intelligence 2.1, 3.1, 3.4, 4.2, 4.4, 4.6, 9.2
- Asylum 6.7.1, 8.5

- BfV (Federal Office for the Protection of the Constitution) 6.5, 6.7.1, 6.7.4, 6.7.5
- Binding Corporate Rules (BCR) 3.2, 10.1
- Biometrics 2.1, 3.2, 6.2,
- BMWi - Federal Ministry for Economic Affairs and Energy 6.7.4
- Brexit 3.2, 8.1, 8.1.1
- Bundestag police 7.2

- Case handling system 6.3
- Census 5.4
- Central Aliens Register (Ausländerzentralregister, AZR) 8.5
- Central service provider 6.3, 6.7.3
- Cloud Act 6.1.1
- Commercial enterprises 2.2, 5.1
- Complaints 4.3, 4.5, 5.1, 8.1.3, 8.3, 8.5, 9.3
- Consent 2.1, 3.2, 4.2.2, 4.5, 4.6, 5.1, 8.2, 8.3, 8.4, 8.7
- Consistency mechanism 3.1, 3.2
- Convention108 3.3
- Cookies 4.5.2
- Corrective actions 8.9, 9.3
- Council of Europe 3.3, 6.1.3
- Customs investigation 5.3.1, 8.5
- Customs Investigation Service Act (ZfdG) 5.3.1
- Cyber attack 5.5, 8.2, 8.7
- Cybercrime 6.1.3

- Dark web 5.3.3
- Data breach 9.3
- Data Ethics Commission (DEK) 4.4, 4.6
- Data Exchange Improvement Act 8.5
- Data minimisation 4.2, 4.3,
- Data Protection Conference, german (DSK) 3.1, 4.1, 4.2.1, 4.4, 4.5.1, 5.5, 8.5, 8.6, 8.7, 8.9, 8.10, 8.12
- international 3.4, 4.4
- Data protection impact assessment 4.2.1, 5.6, 10.2
- Data protection officer 2.2, 3.1, 5.1
- Data sovereignty 4.5.1, 8.7
- Data transfers 3.2, 5.1, 5.3.1, 8.3, 8.12
- Database 3.2, 5.6, 6.2
- Driving, automated 8.7
- Driving, connected 8.7

- eEvidence Regulation 6.1.2
- Employee data protection 2.3
- Encryption 5.3.3, 8.3, 8.8.1
- ePrivacy Regulation 2.2, 3.2, 5.2
- EURODAC 2.2, 6.7.1
- European Commission 2.2, 4.1, 5.2, 6.1.2, 8.1.2, 8.7
- European Court of Justice (ECJ) 6.4, 8.1.3
- European Data Protection Board (EDPB) 3.2, 4.1, 6.1.1, 8.1.2, 8.1.3, 8.9
- European Data Protection Supervisor 3.2
- European Data Protection Supervisor 3.2
- EU-US Privacy Shield 3.2, 8.1.2, 8.1.3
- Evaluation 3.1, 3.3, 4.1, 5.3

- Facebook 2.2, 3.4, 8.1.2, 8.4
- Facial recognition 6.2
- Fanpage 2.2, 8.6
- Federal Client (Bundesclient) 8.11, 8.12
- Federal Cloud (Bundescloud) 8.11
- Federal Criminal Police Office (BKA) 2.2, 2.3, 6.3, 6.4, 6.7.1, 6.7.2, 6.7.3, 7.2
- Federal Data Protection Act 2.2, 2.3, 5.1
- Federal Employment Agency's Job Board 8.4
- Federal Intelligence Service (BND) 2.3, 6.6, 6.7.1, 6.7.5
- Federal IT Consolidation Project 8.11
- Federal Network Agency (Bundesnetzagentur) 5.2, 9.1
- Federal Police 6.2, 6.7.1
- Fines 4.1, 5.1, 8.9, 9.1

- G10 Commission 2.2, 6.7.5
- GDPR 2.3, 3.2, 4.1, 5.1
- General Data Protection Regulation (GDPR) 2.3, 3.2, 4.1, 5.1

German Bundestag 2.2, 2.3, 7.1, 7.2, 11
 Global Privacy Assembly 3.4

Health record 2.1, 4.2.1

Internal pass 7.1, 7.2
 International Conference of Data Protection and
 Privacy Commissioners 3.4
 Interoperability 3.2, 4.2.1, 4.6
 ISO/IEC-17065 8.10
 IT Service Provider 8.11

Job Board 8.4
 Job centre 2.2, 4.3

Law Enforcement Directive 5.3.1, 7.2
 Legislation 5.1 ff.

Mandatory controls 5.3.1, 6.7.1
 Messenger services 4.2, 4.6
 Misuse of data 4.6, 8.4
 Modernisation of registers 2.1, 5.5
 Motor vehicles 8.7

Number plate recognition 3.1, 8.7

Omnibus Act 5.1
 Online Access Act 8.2

Passenger name records (PNR) 6.4
 Passenger Name Records (PNR) 2.2, 6.4
 Patient data 3.1, 4.2.1
 Pilot project 6.2, 8.8.2
 Police 2020 6.3
 Police Acts 6.7.3
 Post 8.8 ff.
 Postal secrecy 8.8
 Powers
 (supervisory) 2.2, 2.3, 4.1, 4.3, 5.2, 5.6, 8.9
 (others) 5.3, 5.3.1, 5.3.3, 6.7.2, 7.2, 8.1.2
 Privacy by Default 8.7
 Privacy by Design 8.7
 Processors pursuant 2.2, 3.1
 Public outreach work 9.2

Reporting obligation 4.2.2, 5.6
 Resolution 3.1, 3.4
 Right-wing extremism file 2.2, 6.7.1

Sanction (others) 2.2, 4.1, 5.1, 8.9
 Sanctioning principles 8.9
 Schengen Information System 3.2, 6.7.1
 Schrems II 8.1.2, 8.1.3

Security clearance 6.7.4
 Security of processing 8.3
 Short paper, DSK 3.1
 Single contact point 10.1, 10.2
 Source telecommunications surveillance 6.7.2
 Supervisory 6.7.5, 8.1.3

Telecommunications Act 2.1, 5.1, 5.2, 8.1.1
 Telematics 2.1, 4.2, 4.2.1, 5.6, 8.7
 Third-country transfers 8.1
 Tracking 3.2, 4.2, 4.5.2, 5.3.3, 5.6

Windows 10 3.1, 8.12
 WLAN 5.3.1